

#3

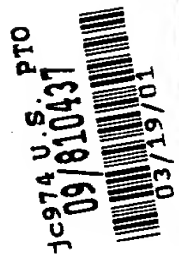
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Tsutomu MATSUMOTO, et al.**

Serial No.: **Not Yet Assigned**

Filed: **March 19, 2001**

For: **CARD SETTLEMENT METHOD AND SYSTEM USING MOBILE INFORMATION  
TERMINAL**



**CLAIM FOR PRIORITY UNDER 35 U.S.C. 119**

Commissioner for Patents  
Washington, D.C. 20231

March 19, 2001

Sir:

The benefit of the filing date of the following prior foreign application is hereby requested for the above-identified application, and the priority provided in 35 U.S.C. 119 is hereby claimed:

**Japanese Appln. No. 2000-358016, filed November 24, 2000**

In support of this claim, the requisite certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the applicants have complied with the requirements of 35 U.S.C. 119 and that the Patent and Trademark Office kindly acknowledge receipt of said certified copy.

In the event that any fees are due in connection with this paper, please charge our Deposit Account No. 01-2340.

Respectfully submitted,  
ARMSTRONG, WESTERMAN, HATTORI  
McLELAND & NAUGHTON LLP

A large, stylized handwritten signature in black ink is written over the typed name of William F. Westerman.

William F. Westerman  
Reg. No. 29,988

Atty. Docket No.: 010369  
Suite 1000, 1725 K Street, N.W.  
Washington, D.C. 20006  
Tel: (202) 659-2930  
Fax: (202) 887-0357  
WFW/ll

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

Jc974 U.S. PTO  
09/810437  
03/19/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application:

2000年11月24日

出 願 番 号  
Application Number:

特願2000-358016

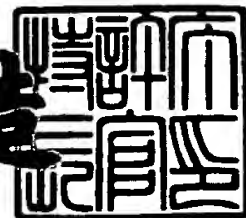
出 願 人  
Applicant(s):

富士通株式会社

2001年 1月26日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



出証番号 出証特2001-3000063

【書類名】 特許願

【整理番号】 0051073

【提出日】 平成12年11月24日

【あて先】 特許庁長官 及川 耕造 殿

【国際特許分類】 G06F 15/30 340  
G11C 7/00 315  
H04B 1/034

【発明の名称】 携帯情報端末を利用したカード決済方法及びシステム

【請求項の数】 18

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 松本 勉

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 光本 弘樹

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 鎌田 武志

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100077517

【弁理士】

【氏名又は名称】 石田 敬

【電話番号】 03-5470-1900

【選任した代理人】

【識別番号】 100092624

【弁理士】

【氏名又は名称】 鶴田 準一

【選任した代理人】

【識別番号】 100100871

【弁理士】

【氏名又は名称】 土屋 繁

【選任した代理人】

【識別番号】 100082898

【弁理士】

【氏名又は名称】 西山 雅也

【選任した代理人】

【識別番号】 100081330

【弁理士】

【氏名又は名称】 樋口 外治

【手数料の表示】

【予納台帳番号】 036135

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9905449

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 携帯情報端末を利用したカード決済方法及びシステム

【特許請求の範囲】

【請求項 1】 店舗における取引の決済に、ＩＣカード読み書き機能と無線通信機能とを備えた携帯情報端末を利用するカード決済方法であって、

店舗を利用中の顧客により前記携帯情報端末が無線によりネットワーク経由で認証サーバに接続される段階と、

前記顧客により自分のＩＣカードが前記携帯情報端末に装着され、このＩＣカードに格納されている情報が読み取られて前記認証サーバに送られる段階と、

前記ＩＣカードに格納されてカードの正当性を証明する認証情報、少なくともカード番号を含む決済情報、及び顧客により入力されて顧客の正当性を証明する暗証情報から、前記認証サーバにより今回の取引の認証が判断される段階と、

今回の取引の認証後に、決済サーバから発行された一時的なパスワードが前記携帯情報端末に送られて表示される段階と、

一時的なパスワードと今回の取引情報が店舗側の決済端末から入力されて前記決済サーバに送られる段階と、

前記パスワードと取引情報が決済条件を満たした取引について、前記決済サーバにより決済が行われる段階と、

を備えることを特徴とする携帯情報端末を利用したカード決済方法。

【請求項 2】 店舗における取引の決済に、ＩＣカード読み書き機能と無線通信機能とを備えた携帯情報端末を利用するカード決済方法であって、

店舗を利用中の顧客により前記携帯情報端末が無線によりネットワーク経由で認証サーバに接続される段階と、

前記顧客により自分のＩＣカード及び前記店舗に備えられた店舗用ＩＣカードが前記携帯情報端末に装着され、これらのＩＣカードに格納されている情報が読み取られて前記認証サーバに送られる段階と、

前記顧客のＩＣカードに格納されて顧客の正当性を証明する認証情報と前記店舗用ＩＣカードに格納されて店舗を特定する店舗情報から、前記認証サーバによりこれらのＩＣカードの適否が前記認証サーバにより判断される段階と、

これらのＩＣカードが認証された後に、顧客から入力されて顧客の正当性を証明する暗証情報により、前記顧客の認証が前記認証サーバにより行われる段階と

顧客が認証された後に、顧客のＩＣカードに格納されている少なくともカード番号を含む決済情報と顧客により入力された今回の取引情報により、決済サーバにより今回の取引の認証が判断される段階と、

今回の取引が決済条件を満たしたと判断された場合に、前記決済サーバにより決済が行われる段階と、

を備えることを特徴とする携帯情報端末を利用したカード決済方法。

【請求項３】 店舗における取引の決済に、ＩＣカード読み書き機能と近距離無線通信機能とを備えた携帯情報端末と、近距離無線通信機能を備えた店舗側の決済端末を利用するカード決済方法であって、

店舗を利用中の顧客により前記携帯情報端末が無線により店舗側の決済端末に接続される段階と、

前記顧客により自分のＩＣカードが前記携帯情報端末に装着され、このＩＣカードに格納されている情報と、前記顧客から入力されて顧客の正当性を証明する暗証情報が前記決済端末に送られる段階と、

ＩＣカードに格納されていたカードの正当性を証明する認証情報と前記暗証情報が、前記決済端末から決済ネットワークを通じて認証サーバに送られる段階と

前記認証情報と暗証情報に基づき、前記認証サーバにより、前記ＩＣカードの適否と前記顧客の適否が判断される段階と、

前記ＩＣカードと前記顧客が認証された後、前記顧客によりＩＣカードに格納された少なくともカード番号を含む決済情報、及び顧客により入力された取引情報が無線により前記店舗側の決済端末に入力される段階と、

前記決済端末が今回の取引の有効性を判断する段階と、

有効性の確認後、前記決済端末から今回の取引情報が店舗を特定する店舗情報と共に前記決済ネットワーク経由で決済サーバに送られる段階、及び、

前記決済サーバにより決済が行われる段階と、

を備えることを特徴とする携帯情報端末を利用したカード決済方法。

【請求項 4】 請求項 1 から 3 の何れか 1 項に記載の携帯情報端末を利用したカード決済方法であって、更に、前記決済サーバにより前記決済が実行された後に、前記店舗側の決済端末から利用明細が発行されることを特徴とするカード決済方法。

【請求項 5】 店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

携帯情報端末に設けられ、カードの正当性を証明する認証情報、顧客の正当性を証明する暗証情報、及び、少なくともカード番号を含む決済情報が格納された IC カードに対して情報の読み書きを行う IC カードの読み書き機能、

特定サービス用のアプリケーションソフトウェアの格納、前記携帯情報端末の画面の制御、及び、前記携帯情報端末のネットワークと前記決済ネットワークの間のゲートウェイ機能を提供するアプリケーションサーバ、及び、

前記 IC カードから前記携帯情報端末のネットワーク、前記アプリケーションサーバ、及び、前記決済ネットワークを通じて入力された決済情報を基に、一時的なパスワードを発行する、前記決済サーバに設けられたパスワード発行機能とを備えることを特徴とする決済システム。

【請求項 6】 請求項 5 に記載の携帯情報端末を利用したカード決済システムであって、店舗において顧客に代金支払いが発生した際に、以下の手順、

顧客により前記 IC カードが装着された前記携帯情報端末が、前記アプリケーションサーバを経由して前記認証サーバに接続され、この IC カードに格納された認証情報が前記認証サーバに送出される、

前記 IC カードに格納された認証情報に基づき、前記認証サーバによりこの IC カードの適否が判断される、

前記カードが適切であると認証された後、顧客により前記携帯情報端末の入力装置から暗証情報が入力されて前記認証サーバに送られる、

暗証情報により顧客が確認された後、顧客により前記 IC カードに格納された決済情報が入力されて前記決済サーバに送られる、

前記暗証情報、決済情報、並びに受信時間を基にして、前記決済サーバにより発行された一時的なパスワードが前記携帯情報端末に送られ、その表示器に表示される、

表示された一時的なパスワードと今回の売上情報が前記店舗に設置された前記決済端末から入力される、及び、

前記一時的なパスワードと取引情報が前記決済サーバによりチェックされた後、決済条件を満たした取引について、前記決済サーバからの信号により、前記店舗の決済端末から利用明細が発行される、

により決済が行なわれることを特徴とする携帯情報端末を利用したカード決済システム。

【請求項 7】 店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

携帯情報端末に設けられ、少なくともカード番号、カードの有効期限、及び顧客名を含む決済情報が格納された個人用 IC カード、及び、少なくとも取引加盟店 ID を含む店舗情報が格納された店舗用 IC カード、に対して情報の読み書きを行う IC カードの読み書き機能、及び、

特定サービス用のアプリケーションソフトウェアの格納、前記携帯情報端末の画面の制御、及び、前記携帯情報端末のネットワークと前記決済ネットワークの間のゲートウェイ機能を提供するアプリケーションサーバと、

を備えることを特徴とする決済システム。

【請求項 8】 請求項 7 に記載の携帯情報端末を利用したカード決済システムであって、店舗において顧客に代金支払いが発生した際に、以下の手順、

前記個人用と店舗用の IC カードが装着された前記携帯情報端末が、前記アプリケーションサーバを経由して前記認証サーバに接続され、2 つの IC カードに格納された個々のカードの正当性を証明する認証情報がそれぞれ前記認証サーバに送出される、

前記 IC カードに格納された認証情報に基づき、前記認証サーバにより 2 つの IC カードの適否が判断される、



前記 2 つの IC カードが適切であると認証された後、顧客により前記携帯情報端末の入力装置から暗証情報が入力されて前記認証サーバに送られる、

暗証情報により顧客が確認された後、前記個人用 IC カードに格納された決済情報、及び店舗用 IC カードに格納された店舗情報と共に前記決済サーバに送られる、及び、

前記決済サーバにより前記決済情報、店舗情報、及び取引情報をチェックされた後、決済条件を満たした取引について、前記決済サーバからの信号により、前記店舗の決済端末から利用明細が発行される、

により決済が行なわれることを特徴とする携帯情報端末を利用したカード決済システム。

【請求項 9】 請求項 5 または 7 に記載の携帯情報端末を利用したカード決済システムにおいて、

前記アプリケーションサーバが前記携帯情報端末のネットワークと前記決済ネットワークの間に位置するサービスセンタに設けられており、このサービスセンタに前記認証サーバが設けられていることを特徴とするカード決済システム。

【請求項 10】 請求項 5 または 7 に記載の携帯情報端末を利用したカード決済システムにおいて、

前記認証サーバに相当する認証機能が前記携帯情報端末に設けられており、前記 IC カードの適否の認証が前記携帯情報端末において行なわれることを特徴とするカード決済システム。

【請求項 11】 店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

顧客の所有する携帯情報端末に設けられた無線モジュール、

携帯情報端末に設けられて、少なくともカード番号、カードの有効期限、及び顧客名を含む決済情報が格納された IC カードに対して情報を読み書きする IC カードの読み書き機能、及び、

前記携帯情報端末の無線モジュールと交信を行なうことができる前記決済端末に設けられた無線モジュールとを備えることを特徴とする決済システム。

【請求項 1 2】 請求項 1 1 に記載の携帯情報端末を利用したカード決済システムであって、店舗において顧客に代金支払いが発生した際に、以下の手順、

顧客により前記 IC カードが装着された前記携帯情報端末が、前記無線モジュールを介して前記店舗の決済端末に接続され、前記 IC カードに格納されてカードの正当性を証明する認証情報と顧客の入力した顧客の正当性を証明する暗証情報が前記決済端末に送出される、

前記決済端末から前記 IC カードに格納された認証情報と顧客の入力した暗証情報が前記決済ネットワークを介して前記認証サーバに送出される、

前記認証情報と暗証情報に基づき、前記認証サーバによりこの IC カードの適否と利用者の適否が判断される、

前記 IC カードと利用者が認証された後、前記 IC カードに格納された決済情報、及び入力された取引金額情報と商品情報、が前記無線モジュールを介して前記決済端末に送出される、

前記決済端末により商品と金額の有効性が審査される、

有効性の確認後、前記決済端末から前記決済情報、取引金額情報、及び、店舗情報が前記決済ネットワークを経由して前記認証サーバ経由で前記決済サーバに送出される、及び、

受け取った前記決済情報、取引金額情報、及び、店舗情報を基に前記決済サーバにより当該取引の有効性が審査され、その結果と利用明細が前記決済ネットワーク経由で前記決済端末に送付され、前記店舗の決済端末から利用明細が発行される、

により決済が行なわれることを特徴とする携帯情報端末を利用したカード決済システム。

【請求項 1 3】 請求項 1 2 に記載の携帯情報端末を利用したカード決済システムにおいて、

前記決済ネットワークと前記決済端末の間にアプリケーションサーバが設けられており、前記認証サーバがこのアプリケーションサーバに設置されていることを特徴とするカード決済システム。

【請求項 1 4】 請求項 1 1 に記載の携帯情報端末を利用したカード決済システムにおいて、

1 台の前記決済端末が前記無線モジュールを介して同時に複数台の携帯情報端末と決済処理が実行できるようになっているカード決済システム。

【請求項 1 5】 請求項 4 に記載の携帯情報端末を利用したカード決済方法において、

前記決済サーバにより前記店舗の決済端末から利用明細が発行される際に、前記アプリケーションサーバ経由で前記携帯情報端末の表示器にも決済結果が表示されることを特徴とするカード決済システム。

【請求項 1 6】 請求項 5 に記載の携帯情報端末を利用したカード決済システムにおいて、

ＩＣカードの読み書き機能が前記携帯情報端末に外付けされているカード決済システム。

【請求項 1 7】 請求項 5 に記載の携帯情報端末を利用したカード決済システムにおいて、

ＩＣカードの読み書き機能が前記携帯情報端末に内蔵されているカード決済システム。

【請求項 1 8】 請求項 5 に記載の携帯情報端末を利用したカード決済システムにおいて、

前記携帯情報端末が携帯電話であるカード決済システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は携帯情報端末を利用したカード決済方法及びシステムに関し、特に、ＩＣカードに対して読み書きが可能な携帯情報端末を利用して、無線により購入代金や利用代金の決済を行なうことができるカード決済方法及びシステムに関する。

【 0 0 0 2 】

【従来の技術】

従来、顧客が店舗を利用した際に発生した料金（購入代金、飲食代金、サービス利用代金等）をキャッシュレスで決済する方法として、クレジットカードやデビットカードが普及している。クレジットカードは銀行と商店が提携して行なう信用販売制度に使用するカードであり、銀行に預金口座がある人に対して発行され、クレジット会社が関与している。クレジットカードを使用して代金の決済を行なう場合は、店舗に設置された決済端末であるC A T端末にクレジットカードの磁気ストライプを読み込ませて決済情報をクレジット会社に送るようになっている。

【0003】

クレジットカードは直接顧客の銀行口座とは結びついていないので、C A T端末からクレジットカードの認証センタに利用者のカード利用を認証しても良いかどうかを問い合わせ（磁気情報を送る）、認証センタがその情報から認証の良否を判断する。認証センタはクレジットカードから読み取られた磁気情報の内容を確認し、カード番号が顧客ブラックリストに載っていないか、または、カードの利用額を越えていないか等をチェックして不正を防止する。このチェックによりクレジットカードに問題がなければ、認証センタからC A T端末に認証が返信される。そうすると、クレジットカード利用日の20日～50日後に伝票が上がって顧客の銀行口座から顧客の利用金額が引かれるようになっている。

【0004】

このように、クレジットカードによる決済では、店舗の利用日の20日～50日後に利用代金が顧客の銀行口座から引き落とされる。一方、近年、信用力の低い人にも発行されるカードシステムであり、即時、もしくは2～3日以内に決済されるカードシステムであるデビットカードが普及し始めている。デビットカードはクレジット会社のネットワークを経由して銀行のホストコンピュータに接続されている。デビットカードは顧客の銀行の口座と直結しているので、支払いが発生したその場で顧客の預金口座から代金が引き落とされる。

【0005】

ところが、このようなクレジットカードやデビットカードは、カード上の磁気ストライプに決済に必要な情報を記録したものが一般的であり、第三者による磁

気データの不正取得によるカードの不正使用や、磁気ストライプ上のデータの改ざんに対しては、対抗する術がなかった。

この問題を解決すべく登場したのが磁気カードに比べてはるかに大容量、かつカードの中の情報を覗き見られることのない、対タンパー性を備えたＩＣカードである。このＩＣカードはプラスチックカードの内部にＩＣを埋め込んだものであり、欧米ではスマートカードと呼ばれるものである。ＩＣカードは基本的にはＣＰＵ、ＲＯＭ、ＥＥＰＲＯＭ等を内蔵しており、メモリからの情報の入出力をＣＰＵで管理するものである。ＩＣカードは利用者本人のみ知りうる暗証番号で保護されており、第三者による不正使用を防ぐようになっている。また、暗証番号の代わりとして、指紋、音声、虹彩などの生体情報を認証手段として用いることにより、一層のセキュリティの向上を図るようにしたＩＣカードもある。

【０００６】

【発明が解決しようとする課題】

しかしながら、前述のようなＩＣカードの普及には、店舗にＩＣカード読み取り機能付きの端末を設置する必要があり、それには多額に費用が発生するため、ＩＣカードリーダーの設置コストの価格がＩＣカードの普及の阻害要因となっているという問題点があった。

【０００７】

そこで、本発明は、店舗側のＣＡＴ端末はそのままにしておいて、ＩＣカードを利用して決済を行なうことができる携帯情報端末を利用したカード決済方法及びシステムを提供することを目的としている。

【０００８】

【課題を解決するための手段】

前記目的を達成する本発明の方法は、以下に第１から第３の発明として示される。

第１の発明は、店舗における取引の決済に、ＩＣカード読み書き機能と無線通信機能とを備えた携帯情報端末を利用するカード決済方法であって、

店舗を利用中の顧客により携帯情報端末が無線によりネットワーク経由で認証サーバに接続される段階と、顧客により自分のＩＣカードが携帯情報端末に装着

され、このＩＣカードに格納されている情報が読み取られて認証サーバに送られる段階と、ＩＣカードに格納されてカードの正当性を証明する認証情報、少なくともカード番号を含む決済情報、及び顧客により入力されて顧客の正当性を証明する暗証情報から、認証サーバにより今回の取引の認証が判断される段階と、今回の取引の認証後に、決済サーバから発行された一時的なパスワードが携帯情報端末に送られて表示される段階と、一時的なパスワードと今回の取引情報が店舗側の決済端末から入力されて決済サーバに送られる段階と、パスワードと取引情報が決済条件を満たした取引について、決済サーバにより決済が行われる段階とを備えることを特徴としている。

## 【 0 0 0 9 】

第２の発明は、店舗における取引の決済に、ＩＣカード読み書き機能と無線通信機能とを備えた携帯情報端末を利用するカード決済方法であって、

店舗を利用中の顧客により携帯情報端末が無線によりネットワーク経由で認証サーバに接続される段階と、顧客により自分のＩＣカード及び店舗に備えられた店舗用ＩＣカードが携帯情報端末に装着され、これらのＩＣカードに格納されている情報が読み取られて認証サーバに送られる段階と、顧客のＩＣカードに格納されて顧客の正当性を証明する認証情報と店舗用ＩＣカードに格納されて店舗を特定する店舗情報から、認証サーバによりこれらのＩＣカードの適否が認証サーバにより判断される段階と、これらのＩＣカードが認証された後に、顧客から入力されて顧客の正当性を証明する暗証情報により、顧客の認証が認証サーバにより行われる段階と、顧客が認証された後に、顧客のＩＣカードに格納されている少なくともカード番号を含む決済情報と顧客により入力された今回の取引情報により、決済サーバにより今回の取引の認証が判断される段階と、今回の取引が決済条件を満たしたと判断された場合に、決済サーバにより決済が行われる段階とを備えることを特徴としている。

## 【 0 0 1 0 】

第３の発明は、店舗における取引の決済に、ＩＣカード読み書き機能と近距離無線通信機能とを備えた携帯情報端末と、近距離無線通信機能を備えた店舗側の決済端末を利用するカード決済方法であって、

店舗を利用中の顧客により携帯情報端末が無線により店舗側の決済端末に接続される段階と、顧客により自分のＩＣカードが携帯情報端末に装着され、このＩＣカードに格納されている情報と、顧客から入力されて顧客の正当性を証明する暗証情報が決済端末に送られる段階と、ＩＣカードに格納されていたカードの正当性を証明する認証情報と暗証情報が、決済端末から決済ネットワークを通じて認証サーバに送られる段階と、認証情報と暗証情報に基づき、認証サーバにより、ＩＣカードの適否と顧客の適否が判断される段階と、ＩＣカードと顧客が認証された後、顧客によりＩＣカードに格納された少なくともカード番号を含む情報、及び顧客により入力された取引情報が無線により店舗側の決済端末に入力される段階と、決済端末が今回の取引の有効性を判断する段階と、有効性の確認後、決済端末から今回の取引情報が店舗を特定する店舗情報と共に決済ネットワーク経由で決済サーバに送られる段階、及び、決済サーバにより決済が行われる段階とを備えることを特徴としている。

#### 【 0 0 1 1 】

以上の方法発明において、決済サーバにより決済が実行された後に、店舗側のクレジット照会用端末から利用明細が発行されるようにすることができる。

また、前記目的を達成する本発明のシステムは、以下に第４から第６の発明として示される。

第４の発明は、店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

携帯情報端末に設けられ、カードの正当性を証明する認証情報、顧客の正当性を証明する暗証情報、及び、少なくともカード番号を含む決済情報が格納されたＩＣカードに対して情報の読み書きを行うＩＣカードの読み書き機能、特定サービス用のアプリケーションソフトウェアの格納、携帯情報端末の画面の制御、及び、携帯情報端末のネットワークと決済ネットワークの間のゲートウェイ機能を提供するアプリケーションサーバ、及びＩＣカードから携帯情報端末のネットワーク、アプリケーションサーバ、及び、決済ネットワークを通じて入力された決済情報を基に、一時的なパスワードを発行する、決済サーバに設けられたパスワ

ード発行機能とを備えることを特徴としている。

【 0 0 1 2 】

第 5 の発明は、店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

携帯情報端末に設けられ、少なくともカード番号、カードの有効期限、及び顧客名を含む決済情報が格納された個人用 IC カード、及び、少なくとも取引加盟店 ID を含む店舗情報が格納された店舗用 IC カードに対して情報の読み書きを行う IC カードの読み書き機能、及び、特定サービス用のアプリケーションソフトウェアの格納、携帯情報端末の画面の制御、及び、携帯情報端末のネットワークと決済ネットワークの間のゲートウェイ機能を提供するアプリケーションサーバとを備えることを特徴としている。

【 0 0 1 3 】

第 6 の発明は、店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

顧客の所有する携帯情報端末に設けられた無線モジュール、携帯情報端末に設けられて、少なくともカード番号、カードの有効期限、及び顧客名を含む決済情報が格納された IC カードに対して情報を読み書きする IC カードの読み書き機能、及び、携帯情報端末の無線モジュールと交信を行なうことができる決済端末に設けられた無線モジュールとを備えることを特徴としている。

【 0 0 1 4 】

第 1 と第 4 の発明では、IC カードによる決済処理を顧客の携帯情報端末で処理させ、処理結果である決済承認結果と一時的なパスワードを店舗のクレジット照会用端末に送付して、店舗のクレジット照会用端末から一時的なパスワードを再入力させることにより、店舗のクレジット照会用端末に何ら IC カード読み書き機能を付加することなく IC カードによる決済を実現できる。この結果、顧客は IC カードによる決済の安全性と、手持ちの携帯情報端末で決済が可能となることによる利便性を得ることができる。



## 【 0 0 1 5 】

第 2 と第 5 の発明では、ＩＣカードによる決済処理を顧客の携帯情報端末で処理させ、かつ、店舗情報も併せて顧客の携帯情報端末で決済サーバに送信することにより、店舗側に決済端末が存在しない場合でも、ＩＣカードによる決済を実現できる。この結果、顧客はＩＣカードによる決済の安全性と、手持ちの携帯情報端末で決済が可能となることによる利便性、及び、店舗側に決済端末が存在しない場合でもＩＣカードによる決済の利便性を得ることができる。

## 【 0 0 1 6 】

第 3 と第 6 の発明では、顧客の携帯情報端末から決済に必要な情報を入力するので、情報の漏洩対策として有効である。また、顧客のカード決済情報はＩＣカードを利用するため、ＩＣカードの安全性の恩恵を受けることができ、不正な取引を防止することが可能である。更に、店舗の決済端末は複数の顧客の携帯情報端末を同時接続して並行処理を行なうことができるので、店舗内の決済端末の縮小と顧客の決済待ち時間の短縮を図ることができ、設備縮小と処理効率可を図ることができる。

## 【 0 0 1 7 】

## 【発明の実施の形態】

以下添付図面を用いて本発明の実施形態を具体的な実施例に基づいて詳細に説明する。

図 1 は本発明の第 1、第 2 の実施形態に使用する携帯情報端末の実施例を示すものである。図 1 (a) では、携帯電話型の携帯情報端末（インターネットに接続可能な携帯電話のようなものであるが、以後単に携帯電話と記す）1 にＩＣカード読み書き装置（図 1 では R / W と記載）2 が取り付けられている。また、図 1 (b) では P D A 型の携帯情報端末 3 にＩＣカード読み書き装置 2 が取り付けられている。これらの実施形態では、既存の携帯電話 1 や P D A 型の携帯情報端末 3 にＩＣカード読み書き装置 2 を接続するだけで、これらにＩＣカード内の情報を読み取らせることができる。

## 【 0 0 1 8 】

図 2 は本発明の第 1、第 2 の実施形態に使用する携帯情報端末である携帯電話

1 に接触型の IC カード 4 を組み込む実施例を示すものである。接触型の IC カード 4 はクレジットカードと同じサイズで、データを格納した IC 8 を内蔵しており、物理的な接点を備えている。図 1 (a) の実施例では、携帯電話 1 に設けられた IC カード挿入口 5 に IC カード 4 が差し込まれている。図中の 8 が IC カード 4 に内蔵された IC である。図 1 (b) の実施例では、携帯電話 1 に IC カード挿入口 5 が設けられていると共に、携帯電話 1 に別の IC 9 が内蔵された IC カード 6 が設けられている。そして、IC カード挿入口 5 には IC カード 4 が差し込まれている。図 1 (c) の実施例では、携帯電話 1 に IC カード挿入口 5 は設けられておらず、別の IC 9 が内蔵された IC カード 6 が予め内蔵されているのみである。このように携帯電話 1 に内蔵される IC カード 6 はシムカードと呼ばれる。

#### 【 0 0 1 9 】

図 3 は本発明の第 1、第 2 の実施形態に使用する携帯電話 1 に非接触型の IC カード 7 を組み込む実施例を示すものである。非接触型の IC カード 7 もクレジットカードと同じサイズであり、カード自体にアンテナがあり、IC チップ 8 が内蔵されている。データを読み取る携帯電話 1 の側にもアンテナがあり、電磁誘導方式、或いは静電結合方式により電気を起こしてチップを起動するようになっている。図 3 (a) では携帯電話 1 に設けられた IC カード挿入口 5 に非接触型の IC カード 7 が差し込まれている。また、図 3 (b) では、携帯電話 1 に設けられた IC カード挿入口 5 に非接触型の IC カード 7 が差し込まれていると共に、携帯電話 1 に IC 9 を備えた接触型の IC カード 6 が内蔵されている。

#### 【 0 0 2 0 】

このように、本発明の携帯情報端末を利用したカード決済システムでは、携帯情報端末に IC カードのデータを読み取らせたり、また、IC カードにデータを書き込ませたりすることによって決済を行うようになっており、IC カードには前述の 3 種類の形態がある。よって、ここではこの IC カードと携帯情報端末を使用した本発明のカード決済システムの 3 つの実施形態について、複数の実施例を基に詳細に説明する。

#### (第 1 の実施形態)

図 4 は本発明の携帯情報端末を利用したカード決済システムの第 1 の実施形態における第 1 の実施例を示すシステム構成図を示している。

【 0 0 2 1 】

図 4 において 3 0 は店舗に設置されているクレジット照会用端末である C A T 端末またはデビット端末であり、決済ネットワーク N S を通じてカード会社或いは銀行（以後カード会社／銀行と記す） 4 0 に接続されている。従来、通常のクレジットカードやデビットカードを用いて店舗で買物等の取引を行った場合は、この C A T 端末またはデビット端末 3 0 により顧客のカードが読み取られ、決済ネットワーク N S を通じてカード会社／銀行 4 0 の図示しない認証サーバで認証が得られると、決済サーバ 4 1 により取引の決済が行われる。

【 0 0 2 2 】

また、近年、携帯電話または携帯端末 1 のような携帯情報端末（以後、代表的に携帯電話 1 のみを例にとって説明する）はパケット通信網のような携帯無線端末ネットワーク N R を通じて交信を行うようになっており、インターネットにも接続できるようになってきている。

このような既存のシステムにおいて、本発明の第 1 の実施形態の第 1 の実施例では、携帯電話 1 に内蔵または外付けの I C カード読み書き装置（以後 I C カード R / W と記す） 2 が接続されており、携帯電話 1 により顧客の情報が格納された I C カード 4 に対して情報の読み書きを行えるようになっている。ここでは、携帯電話 1、内蔵または外付け I C カード R / W 2、及び I C カード 4 をまとめて利用者端末 1 0 と呼ぶ。

【 0 0 2 3 】

次に、この実施例では、携帯無線端末ネットワーク N R と決済ネットワーク N S の間に位置し、特定サービス用のアプリケーションソフトウェアの格納、携帯電話 1 の画面の制御、及び、携帯電話 1 のネットワーク N R と決済ネットワーク N S の間のゲートウェイ機能を提供するアプリケーションサーバ 2 1 を備えたサービスセンタ 2 0 が新たに設けられている。そして、このサービスセンタ 2 0 内には、携帯無線端末ネットワーク N R を通じて携帯電話 1 から送られてくる顧客の I C カード 4 の情報から、I C カード 4 の認証及びこの I C カード 4 の利用者

である顧客の認証を行う認証サーバ22が設けられている。認証サーバ22は、カードの有効期限やブラックリスト掲載の有無等、決済アプリケーションから見たカードの有効性をチェックする機能を備えている。

#### 【0024】

更に、第1の実施形態では、カード会社／銀行40の決済サーバ41の中に、ICカード4から携帯情報端末のネットワークNS、アプリケーションサーバ21、及び、決済ネットワークNSを通じて入力される決済情報を基に、1度しか利用できないパスワードであるワンタイムパスワードを発行するワンタイムパスワード発行機能が備えられている。ワンタイムパスワードで管理するのは、カード番号、カードの暗証番号、ワンタイムパスワードの有効期限、ワンタイムパスワードの利用限度額等である。ワンタイムパスワードの管理方法としては、(a) パスワードそのものが前述の決済情報を暗号化したデータで、パスワードそのものは決済サーバで保存せず、CAT端末からパスワードの提示があった都度データを複合化して決済の妥当性をチェックする方法、(b) パスワードそのものは単なる受付番号的なもので、パスワードに付随する決済情報は全てサーバ側で保存しておき、CAT端末からパスワードの提示があった時にサーバで保存されている情報を呼び出して決済処理する方法等が考えられる。

#### 【0025】

以上のように構成された携帯情報端末を利用したカード決済システムの下で、自己のICカード4を読み込みできるICカードR/W2を備えた携帯電話1を備えた顧客が、CAT端末またはデビット端末30を備えた店舗において、商品を購入する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法について、以下に段階を追って説明する。なお、以下に記す段階番号は図4に太線や破線で示すルートに付された番号に一致している。

#### 【0026】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は携帯電話1でサービスセンタ20に電話すると、利用者端末10とサービスセンタ20の認証サーバ22が接続され、携帯電話1の表示窓に「ICカードを読み込ませて下さい」と表示される。

(2) この指示により顧客は自分のＩＣカード４を携帯電話１に読み込ませる。  
図４ではＩＣカード４は携帯電話１と別体になっているが、このときのＩＣカードの形態は図１～図３で説明したように色々ある。ＩＣカード４の情報はサービスセンタ２０の認証サーバ２２に入力される。サービスセンタ２０の認証サーバ２２は顧客のＩＣカード４に格納された認証情報に基づき、ＩＣカード４を認証すると共に、カードの有効期限やブラックリスト掲載の有無をチェックする。

【００２７】

(3) カードの認証後、顧客本人の認証のため、認証サーバ２２から顧客の携帯電話１からのＩＣカード４の暗証番号の入力が要求される。

(4) 顧客は携帯電話１のキーを使用して暗証番号を入力する。この暗証番号により認証サーバ２２は顧客本人を認証する。

なお、この時の認証方法としては、暗証番号以外にも、指紋、声紋、虹彩等の生体の認証情報をこれらの読み取り装置を使用して読み取って照合するようにすれば、一層のセキュリティを図ることができる。

【００２８】

また、暗証番号による利用者の認証の代わりに、利用者のみ知りうる事柄に関する特殊情報を予めＩＣカードに登録しておき、利用者認証時にこの特殊情報を利用者に入力させてＩＣカード内の特殊情報と比較することにより利用者を認証するようにしても、一層のセキュリティを図ることができる。

(5) 顧客の認証後、ＩＣカード４内に格納されたＩＣクレジット（またはＩＣデビット）情報がアプリケーションサーバ２１を経由して、カード会社／銀行４０の決済サーバ４１に送出される。

【００２９】

(6) カード会社／銀行４０の決済サーバ４１は、受け取ったＩＣカード４の暗証番号およびＩＣクレジット（又はＩＣデビット）情報、並びに受け取った時間を基に、生成された時間からある一定時間内（例えば３０分以内）の１度だけの取引にのみ使用可能なワンタイムパスワード（数字または記号）を生成し、アプリケーションサーバ２１を経由して利用者端末１０の携帯電話１に表示する。

【００３０】

(7) 顧客は携帯電話 1 に表示されたワンタイムパスワードを店舗の C A T 端末またはデビット端末 3 0 から入力する。この入力店舗の人が行っても、顧客が直接行っても良い。

(8) C A T 端末またはデビット端末 3 0 は、顧客の取引情報に入力されたワンタイムパスワードを付加した情報を、決済ネットワーク N S を通じてカード会社／銀行 4 0 の決済サーバ 4 1 に転送する。

【 0 0 3 1 】

(9) 決済サーバ 4 1 は取引情報とパスワードをチェックした後、決済条件を満たした取引に対して店舗の C A T 端末またはデビット端末 3 0 にデータを転送してカード利用明細を発行する。これで顧客の取引が成立する。

この取引の成立から所定期間後に、通常のクレジット取引と同様に、顧客の銀行の口座から成立した取引金額が店舗の口座に振り替えられる。

【 0 0 3 2 】

図 5 は、本発明の携帯情報端末を利用したカード決済システムの第 1 の実施形態における第 2 の実施例を示すシステム構成図である。第 2 の実施例が第 1 の実施例と異なる点は、顧客の I C カード 4 の認証を行う認証サーバの設置位置である。即ち、第 1 の実施例ではサービスセンタ 2 0 内に顧客の I C カード 4 の認証を行う認証サーバ 2 2 が設けられていたが、第 2 の実施例ではサービスセンタ 2 0 内ではなく、カード会社／銀行 4 0 内に認証サーバ 4 2 が設けられている点異なる。

【 0 0 3 3 】

従って、第 2 の実施例では、自己の I C カード 4 を読み込みできる I C カード R / W 2 を備えた携帯電話 1 を備えた顧客が、C A T 端末またはデビット端末 3 0 を備えた店舗において、商品を購入する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法は、認証する部分のみが前述の第 1 の実施例と異なる。よって、第 2 の実施例では第 1 の実施例と異なる部分のみ決済方法を説明する。なお、図 5 に太線や破線で示されるルート番号は第 1 の実施例と同様に段階番号を示している。

【 0 0 3 4 】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は携帯電話 1 でサービスセンタ 2 0 に電話すると、利用者端末 1 0 とサービスセンタ 2 0 の認証サーバ 2 2 が接続され、携帯電話 1 の表示窓に「ＩＣカードを読み込ませて下さい」と表示される。

(2) この指示により顧客は自分のＩＣカード 4 を携帯電話 4 に読み込ませる。図 5 でもＩＣカード 4 は携帯電話 1 と別体になっているが、このときのＩＣカードの形態は図 1 ～図 3 で説明したように色々ある。ＩＣカード 4 の情報はサービスセンタ 2 0 のアプリケーションサーバ 2 1 を経由してカード会社／銀行 4 0 内の認証サーバ 4 2 に入力される。認証サーバ 4 2 は顧客のＩＣカード 4 に格納された認証情報に基づき、ＩＣカード 4 を認証すると共に、カードの有効期限やブラックリスト掲載の有無をチェックする。

#### 【 0 0 3 5 】

(3) カードの認証後、顧客本人の認証のため、認証サーバ 4 2 から顧客の携帯電話 1 からの暗証番号の入力が要求される。

(4) 顧客は携帯電話 1 のキーを使用して暗証番号を入力する。この暗証番号により認証サーバ 4 2 は顧客本人を認証する。

(5) ～(9) の段階は第 1 の実施例と同様である。

#### 【 0 0 3 6 】

図 6 は本発明の携帯情報端末を利用したカード決済システムの第 1 の実施形態における第 3 の実施例を示すシステム構成図である。第 3 の実施例が第 1 の実施例と異なる点は、顧客のＩＣカード 4 の認証を行う認証サーバの設置位置である。即ち、第 1 の実施例ではサービスセンタ 2 0 内に顧客のＩＣカード 4 の認証を行う認証サーバ 2 2 が設けられていたが、第 3 の実施例ではサービスセンタ 2 0 内ではなく、利用者端末 1 0 内に認証機能 1 1 が設けられている点が異なる。

#### 【 0 0 3 7 】

従って、第 3 の実施例では、自己のＩＣカード 4 を読み込みできるＩＣカード R/W 2 を備えた携帯電話 1 を備えた顧客が、ＣＡＴ端末またはデビット端末 3 0 を備えた店舗において、商品を購入する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法は、認証する部分のみが前述の第 1 の実施例と異なる。

る。よって、第3の実施例では第1の実施例と異なる部分のみ決済方法を説明する。なお、図6に太線や破線で示されるルート番号は第1の実施例と同様に段階番号を示している。

#### 【0038】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は携帯電話1でサービスセンタ20に電話すると、利用者端末10とサービスセンタ20が接続され、携帯電話1の表示窓に「ICカードを読み込ませて下さい」と表示される。

(2) この指示により顧客は自分のICカード4を携帯電話4に読み込ませる。図6でもICカード4は携帯電話1と別体になっているが、このときのICカードの形態は図1～図3で説明したように色々ある。ICカード4の情報は携帯電話4内の認証機能11に入力される。認証機能11は顧客のICカード4に格納された認証情報に基づき、ICカード4を認証すると共に、カードの有効期限やブラックリスト掲載の有無をチェックする。

#### 【0039】

(3) カードの認証後、顧客本人の認証のため、認証機能11から顧客の携帯電話1からの暗証番号の入力が要求される。

(4) 顧客は携帯電話1のキーを使用して暗証番号を入力する。この暗証番号により認証機能11は顧客本人を認証する。

(5) ～(9) の段階は第1の実施例と同様である。

#### 【0040】

このように、第1の実施形態では、本来は磁気情報を送るCAT端末またはデビット端末30からワンタイムパスワード送ることによって、サービスセンタ20側でワンタイムパスワードの正当性をチェックしてこの取引がOKであると認証することができるので、顧客のICカードを認証したり受け付けたりするしくみが店舗側にない時でも取引が可能である。即ち、本実施形態では、ICカードによる決済処理を利用者端末で処理させ、処理結果であるワンタイムパスワードのみを決済端末であるCAT端末またはデビット端末30から入力させることにより、CAT端末またはデビット端末30に何らICカード読み書き機能を付加することなく、ICカードによる決済を実現することができる。この結果、顧客



にとっては、ＩＣカードによる決済の安全性と、手持ちの携帯情報端末で決済が可能になることの利便性の双方を享受することができる。

（第２の実施形態）

図７は本発明の携帯情報端末を利用したカード決済システムの第２の実施形態における第１の実施例を示すシステム構成図である。なお、第１の実施形態で説明した施設や構成部材と同じ施設や構成部材には第１の実施形態と同じ符号を付してある。

【００４１】

第２の実施形態においても、図７に示すように、店舗には決済ネットワークＮＳを通じてカード会社／銀行４０に接続されたＣＡＴ端末またはデビット端末３０が必要である。また、携帯情報端末である携帯電話がパケット通信網のような携帯無線端末ネットワークＮＲを通じて交信を行うようになっており、インターネットにも接続できるようになってきていることも必要である。

【００４２】

更に、このような既存のシステムにおいて、本発明の第２の実施形態では、第１の実施形態において必要であったＩＣカード４、携帯電話１に内蔵または外付けのＩＣカードＲ／Ｗ２に加えて、店舗用のＩＣカード３１が必要である。そして、携帯電話１は顧客のＩＣカード４に対して情報の読み書きを行えるようになっており、店舗用のＩＣカード３１内の認証情報も読み込めるようになっている。なお、第２の実施形態でも携帯電話１、内蔵または外付けＩＣカードＲ／Ｗ２、及びＩＣカード４をまとめて利用者端末１０と呼ぶ。

【００４３】

次に、第２の実施形態の第１の実施例では、携帯無線端末ネットワークＮＲと決済ネットワークＮＳの間に位置し、特定サービス用のアプリケーションソフトウェアの格納、携帯電話１の画面の制御、及び、携帯電話１のネットワークＮＲと決済ネットワークＮＳの間のゲートウェイ機能を提供するアプリケーションサーバ２１を備えたサービスセンタ２０が第１の実施形態の第１の実施例と同様に新たに設けられている。そして、このサービスセンタ２０内には、携帯無線端末ネットワークＮＲを通じて携帯電話１から送られてくる顧客のＩＣカード４と店

舗用 IC カード 31 の情報から、IC カード 4 と店舗用 IC カード 31 の認証、及びこの IC カード 4 の利用者である顧客の認証、及び、店舗用 IC カード 31 の利用者である店舗の店員の認証を行う認証サーバ 22 が設けられている。認証サーバ 22 は、カードの有効期限やブラックリスト掲載の有無等、決済アプリケーションから見たカードの有効性をチェックする機能を備えている。

#### 【0044】

一方、第 2 の実施形態では、カード会社／銀行 40 の決済サーバ 41 の中にはワンタイムパスワードを発行するワンタイムパスワード発行機能は備えられていない。

以上のように構成された携帯情報端末を利用したカード決済システムの下で、自己の IC カード 4 と店舗用 IC カード 31 を読み込みできる IC カード R/W 2 を備えた携帯電話 1 を備えた顧客が、CAT 端末またはデビット端末 30 を備えた店舗において、商品を購入する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法について、以下に段階を追って説明する。なお、以下に記す段階番号は図 7 に太線で示すルートに付された番号に一致している。

#### 【0045】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は携帯電話 1 でサービスセンタ 20 に電話すると、利用者端末 10 とサービスセンタ 20 の認証サーバ 22 が接続され、携帯電話 1 の表示窓に「あなたの IC カードと店舗の IC カードを読み込ませて下さい」と表示される。

(2) この指示により顧客は自分の IC カード 4 と店舗から借用した店舗用 IC カードを携帯電話 4 に読み込ませる。図 7 でも IC カード 4 は携帯電話 1 と別体になっているが、このときの IC カードの形態は図 1 ～図 3 で説明したように色々ある。顧客の IC カード 4 と店舗用 IC カード 31 の情報はサービスセンタ 20 の認証サーバ 22 に入力される。サービスセンタ 20 の認証サーバ 22 は顧客の IC カード 4 と店舗用 IC カード 31 に格納された認証情報に基づき、IC カード 4 と店舗用 IC カード 31 を認証すると共に、カードの有効期限やブラックリスト掲載の有無をチェックする。

#### 【0046】

(3) カードの認証後、顧客本人及び店舗の店員の認証のため、認証サーバ 2 2 から顧客の携帯電話 1 からの IC カード 4 の暗証番号及び店舗用 IC カード 3 1 の暗証番号の入力が要求される。

(4) 顧客及び店舗の店員は携帯電話 1 のキーを使用して暗証番号を入力する。  
この暗証番号により認証サーバ 2 2 は顧客本人及び店舗の店員を認証する。

【 0 0 4 7 】

なお、この時の認証方法としては、暗証番号以外にも、指紋、声紋、虹彩等の生体の認証情報をこれらの読み取り装置を使用して読み取って照合するようにすれば、一層のセキュリティを図ることができる。

(5) 顧客及び店舗の店員の認証後、IC カード 4 内に格納された IC クレジット（または IC デビット）情報、店舗用 IC カード内に格納された店舗情報に加え、店舗での取引金額がアプリケーションサーバ 2 1 を経由して、カード会社／銀行 4 0 の決済サーバ 4 1 に送出される。

【 0 0 4 8 】

(6) カード会社／銀行 4 0 の決済サーバ 4 1 は、受け取った IC カード 4 の暗証番号、IC クレジット（又は IC デビット）情報、並びに店舗用 IC カード 3 1 の店舗情報、及び、取引金額情報をもとにして、当該取引の有効性を審査し、その結果をアプリケーションサーバ 2 1 を経由して利用者端末 1 0 の携帯電話 1 に表示する。

【 0 0 4 9 】

(7) 決済サーバ 4 1 は同時に、決済条件を満たした取引に対して店舗の C A T 端末またはデビット端末 3 0 にデータを転送してカード利用明細を発行する。これで顧客の取引が成立する。C A T 端末またはデビット端末 3 0 からの利用明細の発行は、店舗側にも取引の控えがないと困るので行うものであるが、必要がない場合には省略することができる。

【 0 0 5 0 】

この取引の成立から所定期間後に、通常のクレジット取引と同様に、顧客の銀行の口座から成立した取引金額が店舗の口座に振り替えられる。

図 8 は本発明の携帯情報端末を利用したカード決済システムの第 2 の実施形態

における第 2 の実施例を示すシステム構成図である。

第 2 の実施例が第 1 の実施例と異なる点は、顧客の IC カード 4 及び店舗用 IC カード 3 1 の認証を行う認証サーバの設置位置である。即ち、第 1 の実施例ではサービスセンタ 2 0 内に顧客の IC カード 4 及び店舗用 IC カード 3 1 の認証を行う認証サーバ 2 2 が設けられていたが、第 2 の実施例ではサービスセンタ 2 0 内ではなく、カード会社／銀行 4 0 内に認証サーバ 4 2 が設けられている点が異なる。

#### 【 0 0 5 1 】

従って、第 2 の実施例では、自己の IC カード 4 と店舗用 IC カード 3 1 を読み込みできる IC カード R/W 2 を備えた携帯電話 1 を備えた顧客が、CAT 端末またはデビット端末 3 0 を備えた店舗において、商品を購入する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法は、認証する部分のみが前述の第 1 の実施例と異なる。よって、第 2 の実施例では第 1 の実施例と異なる部分のみ決済方法を説明する。なお、図 8 に太線で示されるルート番号は第 1 の実施例と同様に段階番号を示している。

#### 【 0 0 5 2 】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は携帯電話 1 でサービスセンタ 2 0 に電話すると、利用者端末 1 0 とサービスセンタ 2 0 の認証サーバ 2 2 が接続され、携帯電話 1 の表示窓に「あなたの IC カードと店舗の IC カードを読み込ませて下さい」と表示される。

(2) この指示により顧客は自分の IC カード 4 と店舗から借用した店舗用 IC カード 3 1 を携帯電話 4 に読み込ませる。図 8 でも IC カード 4 は携帯電話 1 と別体になっているが、このときの IC カードの形態は図 1 ～図 3 で説明したように色々ある。IC カード 4 と店舗用 IC カード 3 1 の情報はサービスセンタ 2 0 のアプリケーションサーバ 2 1 を経由してカード会社／銀行 4 0 内の認証サーバ 4 2 に入力される。認証サーバ 4 2 は顧客の IC カード 4 と店舗用 IC カード 3 1 に格納された認証情報に基づき、IC カード 4 を認証すると共に、カードの有効期限やブラックリスト掲載の有無をチェックする。

#### 【 0 0 5 3 】

(3) カードの認証後、顧客本人及び店舗の店員の認証のため、認証サーバ42から顧客の携帯電話1からの暗証番号の入力が要求される。

(4) 顧客及び店舗の店員は携帯電話1のキーを使用して暗証番号を入力する。この暗証番号により認証サーバ42は顧客本人及び店舗の店員を認証する。

(5) ～(7) の段階は第1の実施例と同様である。

【0054】

図9は本発明の携帯情報端末を利用したカード決済システムの第2の実施形態における第3の実施例を示すシステム構成図である。第3の実施例が第1の実施例と異なる点は、顧客のICカード4及び店舗用ICカード31の認証を行う認証サーバの設置位置である。即ち、第1の実施例ではサービスセンタ20内に顧客のICカード4及び店舗用ICカード31の認証を行う認証サーバ22が設けられていたが、第3の実施例ではサービスセンタ20内ではなく、利用者端末10内に認証機能11が設けられている点が異なる。

【0055】

従って、第3の実施例では、自己のICカード4と店舗用ICカード31を読み込みできるICカードR/W2を備えた携帯電話1を備えた顧客が、CAT端末またはデビット端末30を備えた店舗において、商品を購入する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法は、認証する部分のみが前述の第1の実施例と異なる。よって、第3の実施例では第1の実施例と異なる部分のみ決済方法を説明する。なお、図9に太線で示されるルート番号は第1の実施例と同様に段階番号を示している。

【0056】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は携帯電話1でサービスセンタ20に電話すると、利用者端末10とサービスセンタ20が接続され、携帯電話1の表示窓に「あなたのICカードと店舗用のICカードを読み込ませて下さい」と表示される。

(2) この指示により顧客は自分のICカード4と店舗用のICカード31を携帯電話4に読み込ませる。図9でもICカード4は携帯電話1と別体になっているが、このときのICカードの形態は図1～図3で説明したように色々ある。I

ICカード4と店舗用のICカード31の情報は携帯電話4内の認証機能11に入力される。認証機能11は顧客のICカード4に格納された認証情報に基づき、ICカード4と店舗用のICカード31を認証すると共に、カードの有効期限やブラックリスト掲載の有無をチェックする。

【0057】

(3) カードの認証後、顧客本人及び店舗の店員の認証のため、認証機能11から顧客の携帯電話1からの暗証番号の入力が要求される。

(4) 顧客及び店舗の店員は携帯電話1のキーを使用して暗証番号を入力する。この暗証番号により認証機能11は顧客本人及び店舗の店員を認証する。

(5) ～(7) の段階は第1の実施例と同様である。

【0058】

このように、第2の実施形態では、ICカードによる決済処理を利用者端末で処理させ、かつ店舗情報も合わせて利用者端末より決済サーバに送信することにより、CAT端末またはデビット端末30に何らICカード読み書き機能を付加することなく、ICカードによる決済を実現することができる。また、店舗側にCAT端末またはデビット端末30が存在しない場合でもICカードによる決済を実現することができる。この結果、顧客にとっては、ICカードによる決済の安全性と、手持ちの携帯情報端末で決済が可能になることの利便性の双方を享受することができる。

(第3の実施形態)

図10は本発明の第3の実施形態に使用するICカード4と近距離無線通信モジュール（以後単に無線モジュールという）50とが装着可能な携帯情報端末である携帯電話1の構成を示すものである。無線モジュール50には近距離無線通信の業界標準規格「ブルートゥース」に準拠したものを使用することができる。

このブルートゥースは2.4GHz帯の電波を使用し、データを含んだ信号を79の周波数に分けて送り、受けて側が再合成する通信方式である。使用する周波数を1秒間に1600回変更するために、他の電波やノイズの影響を抑えることができるという長所があり、実用化が進んでいる。また、ブルートゥースは専用の通信チップと超小型アンテナを組み込めば、機器同士が短い信号を出して相

互に確認し、最大 7 台まで無線で機器を接続することができる。

【0059】

図 1 1 は図 1 0 に示す携帯電話 1 と無線モジュール 5 0 の内部構成の実施例を示すものであり、無線モジュール 5 0 は携帯電話 1 に外付けするタイプである。無線モジュール 5 0 の内部には近距離用 R F 部 5 1 とこれに接続する通信インタフェース 5 2、及び図示しない超小型アンテナが組み込まれている。

携帯電話 1 の本体内には C P U 1 2 があり、この C P U 1 2 には、 I C カード R / W 2、遠距離用 R F 部 1 3、入力装置であるキーデバイス 1 4、 R A M や R O M 等のメモリ 1 5、通信インタフェース 1 6 等が接続されている。 I C カード 4 は I C カード R / W 2 に挿入されて格納されているデータが読み取られる。また、無線モジュール 5 0 はその通信インタフェース 5 2 が携帯電話 1 の通信インタフェース 1 6 に接続される。

【0060】

図 1 2 は図 1 0 に示す携帯電話 1 と無線モジュール 5 0 の内部構成の別の実施例を示すものであり、無線モジュール 5 0 は携帯電話 1 に内蔵されるタイプである。無線モジュール 5 0 の内部には近距離用 R F 部 5 1 と図示しない超小型アンテナがあり、近距離用 R F 部 5 1 は携帯電話 1 の C P U 1 2 に直接接続されている。携帯電話 1 側のその他の構成は図 1 1 と同じであるので、同じ構成部材には同じ符号を付してその説明を省略する。

【0061】

図 1 3 は本発明の携帯情報端末を利用したカード決済システムの第 3 の実施形態における第 1 の実施例を示すシステム構成図である。

第 3 の実施形態においては、図 1 3 に示すように、店舗に設置された従来の C A T 端末またはデビット端末 3 0 に、携帯電話 1 に取り付け或いは組み込まれる無線モジュール 5 0 と通信が可能な無線モジュール 7 0 が取り付けられることが必要である。 C A T 端末またはデビット端末 3 0 に無線モジュール 7 0 を加えたものを、ここでは決済端末 6 0 と呼ぶ。決済端末 6 0 は決済ネットワーク N S を通じてカード会社／銀行 4 0 の決済サーバ 4 1 に接続されている。

【0062】

このような既存のシステムにおいて、本発明の第 3 の実施形態では、第 1 の実施形態において必要であった IC カード 4、携帯電話 1 に内蔵または外付けの IC カード R/W 2 に加えて、無線モジュール 5 0 が必要である。そして、携帯電話 1 は顧客の IC カード 4 に対して情報の読み書きを行えるようになっている。なお、第 3 の実施形態でも携帯電話 1、内蔵または外付け IC カード R/W 2、IC カード 4、及び無線モジュール 5 0 をまとめて利用者端末 1 0 と呼ぶ。

#### 【 0 0 6 3 】

更に、第 3 の実施形態の第 1 の実施例では、決済端末 6 0 と決済ネットワーク NS の間に位置し、特定サービス用のアプリケーションソフトウェアの格納等を行うアプリケーションサーバ 2 1 を備えたサービスセンタ 2 0 が新たに設けられている。そして、このサービスセンタ 2 0 内には、決済端末 6 0 から送られてくる顧客の IC カード 4 の情報から、IC カード 4 の認証及びこの IC カード 4 の利用者である顧客の認証を行う認証サーバ 2 2 が設けられている。認証サーバ 2 2 は、カードの有効期限やブラックリスト掲載の有無等、決済アプリケーションから見たカードの有効性をチェックする機能を備えている。

#### 【 0 0 6 4 】

以上のように構成された携帯情報端末を利用したカード決済システムの下で、自己の IC カード 4 を読み込みできる IC カード R/W 2 を備え、無線モジュール 5 0 が取り付け或いは内蔵された携帯電話 1 を備えた顧客が、この無線モジュール 5 0 と交信可能な無線モジュール 7 0 を備えた決済端末 6 0 を備えた店舗において、商品を購入する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法について、以下に段階を追って説明する。なお、以下に記す段階番号は図 1 3 に太線で示すルートに付された番号に一致している。

#### 【 0 0 6 5 】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は自分の IC カード 4 を携帯電話 1 に読み込ませた上で、利用者端末 1 0 の無線モジュール 5 0 と店舗の決済端末 6 0 の無線モジュール 7 0 との間で通信を行う。店舗の決済端末 6 0 はサービスセンタ 2 0 の認証サーバ 2 2 に接続されているので、顧客の IC カード 4 内の認証情報は、店舗の決済端末 6 0 を経由してサービスセンタ 2 0 の認



証サーバ 2 2 に入力される。すなわち、ＩＣカード 4 の正当性を確認するための認証情報が利用者端末 1 0 から店舗の決済端末 6 0 を中継してサービスセンタ 2 0 の認証サーバ 2 2 に送信される。

【 0 0 6 6 】

認証サーバ 2 2 は顧客が本人であるか否かを確認するために、決済端末 6 0 を介して利用者端末 1 0 に暗証番号の入力を要求し、顧客はこの要求に応じて暗証番号を利用者端末 1 0 より入力する。この暗証番号は決済端末 6 0 を介して認証サーバ 2 2 に送信される。

(2) 認証サーバ 2 2 は利用者端末 1 0 のＩＣカード 4 内に格納された認証情報と、顧客が利用者端末から入力した暗証番号に基づき、利用者端末と利用者を認証し、ＩＣカード 4 の認証結果を店舗側決済端末 6 0、無線モジュール 7 0、5 0 を介して利用者端末 1 0 に送信する。

【 0 0 6 7 】

(3) 認証後、利用者端末 1 0 のＩＣカード 4 内に格納されたＩＣクレジット情報（またはＩＣデビット情報）及び店舗での取引金額と商品情報を、顧客が利用者端末 1 0 の入力装置より入力し、ＩＣカード内のデータは無線モジュール 5 0、7 0 により店舗のＣＡＴ端末またはデビット端末 3 0 に送信され、ＣＡＴ端末またはデビット端末 3 0 で商品とその取引金額の有効性を審査する。

【 0 0 6 8 】

(4) 有効性が確認された後、店舗の決済端末 6 0 はＩＣクレジット情報（またはＩＣデビット情報）、店舗での取引金額と商品情報、及び決済端末 6 0 に格納された店舗情報（店舗ＩＤ）をサービスセンタ 2 0 のアプリケーションサーバ 2 1 に送出する。

(5) アプリケーションサーバ 2 1 は利用者端末 1 0 から受け取ったＩＣクレジット情報（またはＩＣデビット情報）、店舗での取引金額と商品情報、及び店舗情報を、決済ネットワーク Ｎ Ｓ を経由してカード会社／銀行 4 0 の決済サーバ 4 1 に転送する。

【 0 0 6 9 】

(6) カード会社／銀行 4 0 の決済サーバ 4 1 は、認証サーバ 2 2 から受け取っ

たＩＣクレジット情報（またはＩＣデビット情報）、店舗情報及び店舗での取引金額情報を基に、当該取引の有効性を審査し、決済条件を満たした取引に対して店舗の決済端末６０にデータを転送してカード利用明細を発行する。これで顧客の取引が成立する。カード利用明細は決済端末６０から無線モジュール７０、５０を介して利用者端末１０にも送られる。

## 【 0 0 7 0 】

この取引の成立から所定期間後に、通常のクレジット取引と同様に、顧客の銀行の口座から成立した取引金額が店舗の口座に振り替えられる。

図１４は本発明の携帯情報端末を利用したカード決済システムの第３の実施形態における第２の実施例を示すシステム構成図である。

第３の実施形態の第２の実施例では、図１４に示すように、ＩＣカード４に読み書きを行うために携帯電話１に内蔵または外付けされたＩＣカードＲ／Ｗ２に加えて、無線モジュール５０が必要であると共に、店舗に設置された従来のＣＡＴ端末またはデビット端末３０に、携帯電話１に取り付け或いは組み込まれる無線モジュール５０と通信が可能な無線モジュール７０が取り付けられることが必要である。

## 【 0 0 7 1 】

第２の実施例でも携帯電話１、内蔵または外付けのＩＣカードＲ／Ｗ２、ＩＣカード４、及び無線モジュール５０をまとめて利用者端末１０と呼ぶと共に、ＣＡＴ端末またはデビット端末３０に無線モジュール７０を加えたものを決済端末６０と呼ぶ。決済端末６０は決済ネットワークＮＳを通じてカード会社／銀行４０の決済サーバ４１に接続されている。第２の実施例では決済端末６０と決済ネットワークＮＳの間にサービスセンタ２０は設けられていない。従って、第２の実施例では、決済サーバ４１と認証サーバ４２は共にカード会社／銀行４０の中に設けられている。

## 【 0 0 7 2 】

以上のように構成された携帯情報端末を利用したカード決済システムの下で、自己のＩＣカード４を読み込みできるＩＣカードＲ／Ｗ２を備え、無線モジュール５０が取り付け或いは内蔵された携帯電話１を備えた顧客が、この無線モジュ

ール50と交信可能な無線モジュール70を備えた決済端末60を備えた店舗において、商品を購入する取引、或いは、所定のサービスを受ける取引を行う場合の決済方法について、図14と図15を用いて段階を追って説明する。なお、図15に記す段階番号は、図14に太線で示すルートに付された番号に一致している。

#### 【0073】

(1) 顧客が店舗で所定の取引を行いたいと思った時、顧客は自分のICカード4を携帯電話1に読み込ませた上で、利用者端末10の無線モジュール50と店舗の決済端末60の無線モジュール70との間で通信を行う。店舗の決済端末60は決済ネットワークNSを通じてカード会社／銀行40の認証サーバ42に接続されているので、顧客のICカード4内の認証情報は、店舗の決済端末60を経由して認証サーバ42に入力される。すなわち、ICカード4の正当性を確認するための認証情報が利用者端末10から店舗の決済端末60を中継して認証サーバ42に送信される。

#### 【0074】

認証サーバ42は顧客が本人であるか否かを確認するために、決済端末60を介して利用者端末10に暗証番号の入力を要求し、顧客はこの要求に応じて暗証番号を利用者端末10に入力する。この暗証番号は決済端末60を介して認証サーバ42に送信される。

(2) 認証サーバ42は利用者端末10のICカード4内に格納された認証情報と、顧客が利用者端末から入力した暗証番号に基づき、利用者端末と利用者を認証し、ICカード4の認証結果を店舗側決済端末60、無線モジュール70、50を介して利用者端末10に送信する。

#### 【0075】

(3) 認証後、利用者端末10のICカード4内に格納されたICクレジット情報（またはICデビット情報）及び店舗での取引金額と商品情報を、顧客が利用者端末10の入力装置より入力し、ICカード内のデータは無線モジュール50、70により店舗の決済端末60に送信され、決済端末60で商品とその取引金額の有効性を審査する。

## 【 0 0 7 6 】

(4) 有効性が確認された後、店舗の決済端末 6 0 は I C クレジット情報（または I C デビット情報）、店舗での取引金額と商品情報、及び決済端末 6 0 に格納された店舗情報（店舗 I D）をカード会社／銀行 4 0 の決済サーバ 4 1 に送出する。

(5) カード会社／銀行 4 0 の決済サーバ 4 1 は、決済端末 6 0 から受け取った I C クレジット情報（または I C デビット情報）、店舗情報及び店舗での取引金額情報を基に、当該取引の有効性を審査し、決済条件を満たした取引に対して店舗の決済端末 6 0 に I C カードデータの認証及び決済された結果と利用明細を送出する。

## 【 0 0 7 7 】

(6) 決済端末 6 0 は決済結果と利用明細を利用者端末 1 0 に送出し、これで顧客の取引が成立する。

この取引の成立から所定期間後に、通常のクレジット取引と同様に、顧客の銀行の口座から成立した取引金額が店舗の口座に振り替えられる。

図 1 6 は本発明の携帯情報端末を利用したカード決済システムの第 3 の実施形態の適用例を示すものである。前述のように、無線モジュール 5 0 にブルートゥースを使用した場合、機器同士が短い信号を出して相互に確認し、最大 7 台まで無線で機器を接続することができる。よって、1 つの店舗において、1 台の決済端末 6 0 をマスターとした場合、スレーブとして無線モジュール 5 0 A ～ 5 0 G を備えた最大 7 台の利用者端末 1 0 A ～ 1 0 G と取引を行うことができる。この場合、各利用者端末 1 0 A ～ 1 0 G を識別するために、無線モジュール間の交信には識別コード A ～ G が追加される。

## 【 0 0 7 8 】

このように第 3 の実施形態でも利用者端末から決済に必要な情報を入力するため、情報の漏洩に対して有効であり、利用者のカード決済情報は I C カードを利用するため、I C カードの安全性の恩恵を受けることができ、不正な取引を防止することが可能である。また、第 3 の実施形態では、複数の利用者端末からの同時接続を可能とし、並行して処理を行うことができるので、店舗内の決済端末の

装置数の削減と顧客の決済待ち時間の短縮が実現でき、設備削減と処理の効率化を図ることができる。

【 0 0 7 9 】

なお、以上の実施例では、携帯情報端末として携帯電話の実施例を説明したが、携帯電話の代わりにインターネットのようなネットワーク網と接続が可能な携帯型のコンピュータを用いても同様の決済を行うことができる。

(付記 1) 店舗における取引の決済に、ＩＣカード読み書き機能と無線通信機能とを備えた携帯情報端末を利用するカード決済方法であって、

店舗を利用中の顧客により前記携帯情報端末が無線によりネットワーク経由で認証サーバに接続される段階と、

前記顧客により自分のＩＣカードが前記携帯情報端末に装着され、このＩＣカードに格納されている情報が読み取られて前記認証サーバに送られる段階と、

前記ＩＣカードに格納されてカードの正当性を証明する認証情報、少なくともカード番号を含む決済情報、及び顧客により入力されて顧客の正当性を証明する暗証情報から、前記認証サーバにより今回の取引の認証が判断される段階と、

今回の取引の認証後に、決済サーバから発行された一時的なパスワードが前記携帯情報端末に送られて表示される段階と、

一時的なパスワードと今回の取引情報が店舗側の決済端末から入力されて前記決済サーバに送られる段階と、

前記パスワードと取引情報が決済条件を満たした取引について、前記決済サーバにより決済が行われる段階と、

を備えることを特徴とする携帯情報端末を利用したカード決済方法。

【 0 0 8 0 】

(付記 2) 店舗における取引の決済に、ＩＣカード読み書き機能と無線通信機能とを備えた携帯情報端末を利用するカード決済方法であって、

店舗を利用中の顧客により前記携帯情報端末が無線によりネットワーク経由で認証サーバに接続される段階と、

前記顧客により自分のＩＣカード及び前記店舗に備えられた店舗用ＩＣカードが前記携帯情報端末に装着され、これらのＩＣカードに格納されている情報が読

み取られて前記認証サーバに送られる段階と、

前記顧客のＩＣカードに格納されて顧客の正当性を証明する認証情報と前記店舗用ＩＣカードに格納されて店舗を特定する店舗情報から、前記認証サーバによりこれらのＩＣカードの適否が前記認証サーバにより判断される段階と、

これらのＩＣカードが認証された後に、顧客から入力されて顧客の正当性を証明する暗証情報により、前記顧客の認証が前記認証サーバにより行われる段階と

顧客が認証された後に、顧客のＩＣカードに格納されている少なくともカード番号を含む決済情報と顧客により入力された今回の取引情報により、決済サーバにより今回の取引の認証が判断される段階と、

今回の取引が決済条件を満たしたと判断された場合に、前記決済サーバにより決済が行われる段階と、

を備えることを特徴とする携帯情報端末を利用したカード決済方法。

【 0 0 8 1 】

（付記 3） 店舗における取引の決済に、ＩＣカード読み書き機能と近距離無線通信機能とを備えた携帯情報端末と、近距離無線通信機能を備えた店舗側の決済端末を利用するカード決済方法であって、

店舗を利用中の顧客により前記携帯情報端末が無線により店舗側の決済端末に接続される段階と、

前記顧客により自分のＩＣカードが前記携帯情報端末に装着され、このＩＣカードに格納されている情報と、前記顧客から入力されて顧客の正当性を証明する暗証情報が前記決済端末に送られる段階と、

ＩＣカードに格納されていたカードの正当性を証明する認証情報と前記暗証情報が、前記決済端末から決済ネットワークを通じて認証サーバに送られる段階と

前記認証情報と暗証情報に基づき、前記認証サーバにより、前記ＩＣカードの適否と前記顧客の適否が判断される段階と、

前記ＩＣカードと前記顧客が認証された後、前記顧客によりＩＣカードに格納された少なくともカード番号を含む情報、及び顧客により入力された取引情報が

無線により前記店舗側の決済端末に入力される段階と、

前記決済端末が今回の取引の有効性を判断する段階と、

有効性の確認後、前記決済端末から今回の取引情報が店舗を特定する店舗情報と共に前記決済ネットワーク経由で決済サーバに送られる段階、及び、

前記決済サーバにより決済が行われる段階と、

を備えることを特徴とする携帯情報端末を利用したカード決済方法。

【 0 0 8 2 】

(付記 4) 付記 1 から 3 の何れか 1 項に記載の携帯情報端末を利用したカード決済方法であって、更に、前記決済サーバにより前記決済が実行された後に、前記店舗側の決済端末から利用明細が発行されることを特徴とするカード決済方法。

(付記 5) 店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

携帯情報端末に設けられ、カードの正当性を証明する認証情報、顧客の正当性を証明する暗証情報、及び、少なくともカード番号を含む決済情報が格納された IC カードに対して情報の読み書きを行う IC カードの読み書き機能、

特定サービス用のアプリケーションソフトウェアの格納、前記携帯情報端末の画面の制御、及び、前記携帯情報端末のネットワークと前記決済ネットワークの間のゲートウェイ機能を提供するアプリケーションサーバ、及び、

前記 IC カードから前記携帯情報端末のネットワーク、前記アプリケーションサーバ、及び、前記決済ネットワークを通じて入力された決済情報を基に、一時的なパスワードを発行する、前記決済サーバに設けられたパスワード発行機能とを備えることを特徴とする決済システム。

【 0 0 8 3 】

(付記 6) 付記 5 に記載の携帯情報端末を利用したカード決済システムであって、店舗において顧客に代金支払いが発生した際に、以下の手順、

顧客により前記 IC カードが装着された前記携帯情報端末が、前記アプリケーションサーバを経由して前記認証サーバに接続され、この IC カードに格納され

た認証情報が前記認証サーバに送出される、

前記ＩＣカードに格納された認証情報に基づき、前記認証サーバによりこのＩＣカードの適否が判断される、

前記カードが適切であると認証された後、顧客により前記携帯情報端末の入力装置から暗証情報が入力されて前記認証サーバに送られる、

暗証情報により顧客が確認された後、顧客により前記ＩＣカードに格納された決済情報が入力されて前記決済サーバに送られる、

前記暗証情報、決済情報、並びに受信時間を基にして、前記決済サーバにより発行された一時的なパスワードが前記携帯情報端末に送られ、その表示器に表示される、

表示された一時的なパスワードと今回の売上情報が前記店舗に設置された前記決済端末から入力される、及び、

前記一時的なパスワードと取引情報が前記決済サーバによりチェックされた後、決済条件を満たした取引について、前記決済サーバからの信号により、前記店舗の決済端末から利用明細が発行される、

により決済が行なわれることを特徴とする携帯情報端末を利用したカード決済システム。

【 0 0 8 4 】

(付記 7) 店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

携帯情報端末に設けられ、少なくともカード番号、カードの有効期限、及び顧客名を含む決済情報が格納された個人用ＩＣカード、及び、少なくとも取引加盟店ＩＤを含む店舗情報が格納された店舗用ＩＣカードに対して情報の読み書きを行うＩＣカードの読み書き機能、及び、

特定サービス用のアプリケーションソフトウェアの格納、前記携帯情報端末の画面の制御、及び、前記携帯情報端末のネットワークと前記決済ネットワークの間のゲートウェイ機能を提供するアプリケーションサーバと、

を備えることを特徴とする決済システム。



【0085】

(付記8) 付記7に記載の携帯情報端末を利用したカード決済システムであって、店舗において顧客に代金支払いが発生した際に、以下の手順、

前記個人用と店舗用のICカードが装着された前記携帯情報端末が、前記アプリケーションサーバを経由して前記認証サーバに接続され、2つのICカードに格納された個々のカードの正当性を証明する認証情報がそれぞれ前記認証サーバに送出される、

前記ICカードに格納された認証情報に基づき、前記認証サーバにより2つのICカードの適否が判断される、

前記2つのICカードが適切であると認証された後、顧客により前記携帯情報端末の入力装置から暗証情報が入力されて前記認証サーバに送られる、

暗証情報により顧客が確認された後、前記個人用ICカードに格納された決済情報、及び店舗用ICカードに格納された店舗情報と共に前記決済サーバに送られる、及び、

前記決済サーバにより前記決済情報、店舗情報、及び取引情報をチェックされた後、決済条件を満たした取引について、前記決済サーバからの信号により、前記店舗の決済端末から利用明細が発行される、

により決済が行なわれることを特徴とする携帯情報端末を利用したカード決済システム。

【0086】

(付記9) 付記5または7に記載の携帯情報端末を利用したカード決済システムにおいて、

前記アプリケーションサーバが前記携帯情報端末のネットワークと前記決済ネットワークの間に位置するサービスセンタに設けられており、このサービスセンタに前記認証サーバが設けられていることを特徴とするカード決済システム。

【0087】

(付記10) 付記5または7に記載の携帯情報端末を利用したカード決済システムにおいて、

前記認証サーバに相当する認証機能が前記携帯情報端末に設けられており、前

記 I C カードの適否の認証が前記携帯情報端末において行なわれることを特徴とするカード決済システム。

【 0 0 8 8 】

(付記 1 1) 店舗に設置された決済端末が決済ネットワークを介してカード会社或いは銀行の保有する認証サーバ及び決済サーバに接続され、顧客がカードを使用して決済を行なえるカード決済システムにおいて、

顧客の所有する携帯情報端末に設けられた無線モジュール、

携帯情報端末に設けられて、少なくともカード番号、カードの有効期限、及び顧客名を含む決済情報が格納された I C カードに対して情報を読み書きする I C カードの読み書き機能、及び、

前記携帯情報端末の無線モジュールと交信を行なうことができる前記決済端末に設けられた無線モジュールとを備えることを特徴とする決済システム。

【 0 0 8 9 】

(付記 1 2) 付記 1 1 に記載の携帯情報端末を利用したカード決済システムであって、店舗において顧客に代金支払いが発生した際に、以下の手順、

顧客により前記 I C カードが装着された前記携帯情報端末が、前記無線モジュールを介して前記店舗の決済端末に接続され、前記 I C カードに格納されてカードの正当性を証明する認証情報と顧客の入力した顧客の正当性を証明する暗証情報が前記決済端末に送出される、

前記決済端末から前記 I C カードに格納された認証情報と顧客の入力した暗証情報が前記決済ネットワークを介して前記認証サーバに送出される、

前記認証情報と暗証情報に基づき、前記認証サーバによりこの I C カードの適否と利用者の適否が判断される、

前記 I C カードと利用者が認証された後、前記 I C カードに格納された決済情報、及び入力された取引金額情報と商品情報、が前記無線モジュールを介して前記決済端末に送出される、

前記決済端末により商品と金額の有効性が審査される、

有効性の確認後、前記決済端末から前記決済情報、取引金額情報、及び、店舗情報が前記決済ネットワークを経由して前記認証サーバ経由で前記決済サーバに

送出される、及び、

受け取った前記決済情報、取引金額情報、及び、店舗情報を基に前記決済サーバにより当該取引の有効性が審査され、その結果と利用明細が前記決済ネットワーク経由で前記決済端末に送付され、前記店舗の決済端末から利用明細が発行される、

により決済が行なわれることを特徴とする携帯情報端末を利用したカード決済システム。

【 0 0 9 0 】

(付記 1 3) 付記 1 2 に記載の携帯情報端末を利用したカード決済システムにおいて、

前記決済ネットワークと前記決済端末の間にアプリケーションサーバが設けられており、前記認証サーバがこのアプリケーションサーバに設置されていることを特徴とするカード決済システム。

【 0 0 9 1 】

(付記 1 4) 付記 1 1 に記載の携帯情報端末を利用したカード決済システムにおいて、

1 台の前記決済端末が前記無線モジュールを介して同時に複数台の携帯情報端末と決済処理が実行できるようになっているカード決済システム。

(付記 1 5) 付記 4 に記載の携帯情報端末を利用したカード決済方法において、

前記決済サーバにより前記店舗の決済端末から利用明細が発行される際に、前記アプリケーションサーバ経由で前記携帯情報端末の表示器にも決済結果が表示されることを特徴とするカード決済システム。

【 0 0 9 2 】

(付記 1 6) 付記 1 から 1 5 の何れか 1 項に記載の携帯情報端末を利用したカード決済システムにおいて、

前記暗証番号による利用者の認証の代わりに、利用者の指紋、声紋、虹彩等の生体情報を生体情報リーダーにより予め IC カードに登録しておき、利用者認証時にこの生体情報リーダーにより生体情報を読み込んで IC カード内の生体情報と比

較することにより利用者を認証するカード決済システム。

【 0 0 9 3 】

（付記 1 7） 付記 1 から 1 5 の何れか 1 項に記載の携帯情報端末を利用したカード決済システムにおいて、

前記暗証番号による利用者の認証の代わりに、利用者のみ知りうる事柄に関する特殊情報を予め IC カードに登録しておき、利用者認証時にこの特殊情報を利用者に入力させて IC カード内の特殊情報と比較することにより利用者を認証するカード決済システム。

【 0 0 9 4 】

（付記 1 8） 付記 5 に記載の携帯情報端末を利用したカード決済システムにおいて、

IC カードの読み書き機能が前記携帯情報端末に外付けされているカード決済システム。

（付記 1 9） 付記 5 に記載の携帯情報端末を利用したカード決済システムにおいて、

IC カードの読み書き機能が前記携帯情報端末に内蔵されているカード決済システム。

【 0 0 9 5 】

（付記 2 0） 付記 5 に記載の携帯情報端末を利用したカード決済システムにおいて、

前記携帯情報端末が携帯電話であるカード決済システム。

【 0 0 9 6 】

【発明の効果】

以上説明したように、本発明の携帯情報端末を利用したカード決済方法及びシステムによれば、以下のような効果がある。

第 1 と第 4 の発明では、IC カードによる決済処理を顧客の携帯情報端末で処理させ、処理結果である決済承認結果とワンタイムパスワードを店舗の決済端末に送付して、店舗の決済端末からワンタイムパスワードを再入力させることにより、店舗の決済端末に何ら IC カード読み書き機能を付加することなく IC カー

ドによる決済を実現できる。この結果、顧客はＩＣカードによる決済の安全性と、手持ちの携帯情報端末で決済が可能となることによる利便性を得ることができる。

【 0 0 9 7 】

第２と第５の発明では、ＩＣカードによる決済処理を顧客の携帯情報端末で処理させ、かつ、店舗情報も併せて顧客の携帯情報端末で決済サーバに送信することにより、店舗側に決済端末が存在しない場合でも、ＩＣカードによる決済を実現できる。この結果、顧客はＩＣカードによる決済の安全性と、手持ちの携帯情報端末で決済が可能となることによる利便性、及び、店舗側に決済端末が存在しない場合でもＩＣカードによる決済の利便性を得ることができる。

【 0 0 9 8 】

第３と第６の発明では、顧客の携帯情報端末から決済に必要な情報を入力するので、情報の漏洩対策として有効である。また、顧客のカード決済情報はＩＣカードを利用するため、ＩＣカードの安全性の恩恵を受けることができ、不正な取引を防止することが可能である。更に、店舗の決済端末は複数の顧客の携帯情報端末を同時接続して並行処理を行なうことができるので、店舗内の決済端末の縮小と顧客の決済待ち時間の短縮を図ることができ、設備縮小と処理効率可を図ることができる。

【図面の簡単な説明】

【図 1】

本発明の第１、第２の実施形態に使用する携帯情報端末の実施例を示すものであり、(a) は携帯電話型の携帯情報端末にＩＣカード読み書き装置が取り付けられた状態を示す図、(b) はＰＤＡ型の携帯情報端末にＩＣカード読み書き装置が取り付けられた状態を示す図である。

【図 2】

本発明の第１、第２の実施形態に使用する携帯情報端末である携帯電話に接触型のＩＣカードを組み込む実施例を示すものであり、(a) は携帯電話に設けられたＩＣカード挿入口にＩＣカードが差し込まれた状態を示す図、(b) は携帯電話に設けられたＩＣカード挿入口にＩＣカードが差し込まれていると共に、携帯電

話に別のＩＣカードが内蔵されている状態を示す図、(c)はＩＣカードが内蔵された携帯電話の例を示す図である。

【図 3】

本発明の第 1、第 2 の実施形態に使用する携帯情報端末である携帯電話に非接触型のＩＣカードを組み込む実施例を示すものであり、(a)は携帯電話に設けられたＩＣカード挿入口に非接触型のＩＣカードが差し込まれた状態を示す図、(b)は携帯電話に設けられたＩＣカード挿入口に非接触型のＩＣカードが差し込まれていると共に、携帯電話に接触型のＩＣカードが内蔵されている状態を示す図である。

【図 4】

本発明の携帯情報端末を利用したカード決済システムの第 1 の実施形態における第 1 の実施例を示すシステム構成図である。

【図 5】

本発明の携帯情報端末を利用したカード決済システムの第 1 の実施形態における第 2 の実施例を示すシステム構成図である。

【図 6】

本発明の携帯情報端末を利用したカード決済システムの第 1 の実施形態における第 3 の実施例を示すシステム構成図である。

【図 7】

本発明の携帯情報端末を利用したカード決済システムの第 2 の実施形態における第 1 の実施例を示すシステム構成図である。

【図 8】

本発明の携帯情報端末を利用したカード決済システムの第 2 の実施形態における第 2 の実施例を示すシステム構成図である。

【図 9】

本発明の携帯情報端末を利用したカード決済システムの第 2 の実施形態における第 3 の実施例を示すシステム構成図である。

【図 1 0】

本発明の第 3 の実施形態に使用するＩＣカードと近距離無線通信モジュールと

が装着可能な携帯情報端末である携帯電話の構成を示す斜視図である。

【図 1 1】

図 1 0 に示す携帯電話と近距離無線通信モジュールの内部構成の一例を示すブロック回路図である。

【図 1 2】

図 1 0 に示す携帯電話と近距離無線通信モジュールの内部構成の別の例を示すブロック回路図である。

【図 1 3】

本発明の携帯情報端末を利用したカード決済システムの第 3 の実施形態における第 1 の実施例を示すシステム構成図である。

【図 1 4】

本発明の携帯情報端末を利用したカード決済システムの第 3 の実施形態における第 2 の実施例を示すシステム構成図である。

【図 1 5】

図 1 4 に示すシステムの無線モジュール間の決済シーケンスを示すシーケンス図である。

【図 1 6】

本発明の携帯情報端末を利用したカード決済システムの第 3 の実施形態の適用例を示すシステム構成図である。

【符号の説明】

- 1 … 携帯電話型の携帯情報端末（携帯電話）
- 2 … IC カード読み書き装置
- 3 … PDA 型の携帯情報端末
- 4 … 接触型の IC カード
- 5 … IC カード挿入孔
- 6 … IC カード
- 7 … 非接触型 IC カード
- 8, 9 … IC
- 10 … 利用者端末

1 1 … 認証機能

2 0 … サービスセンタ

2 1 … アプリケーションサーバ

3 0 … C A T / デビット端末

3 1 … 店舗用 I C カード

4 0 … カード会社 / 銀行

4 1 … 決済サーバ

4 2 … 認証サーバ

5 0 … 無線通信モジュール

6 0 … 決済端末

7 0 … 無線通信モジュール

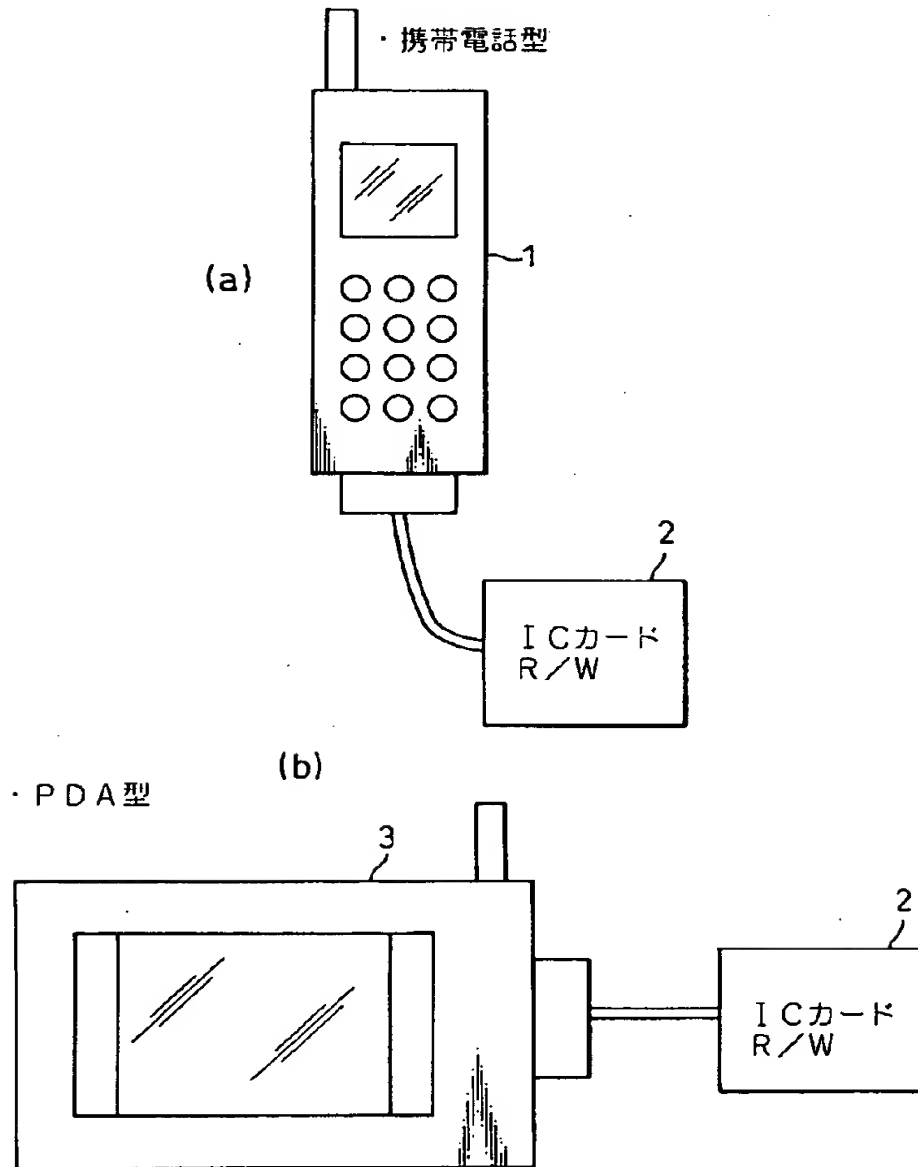


【書類名】 図面

【図 1】

図1

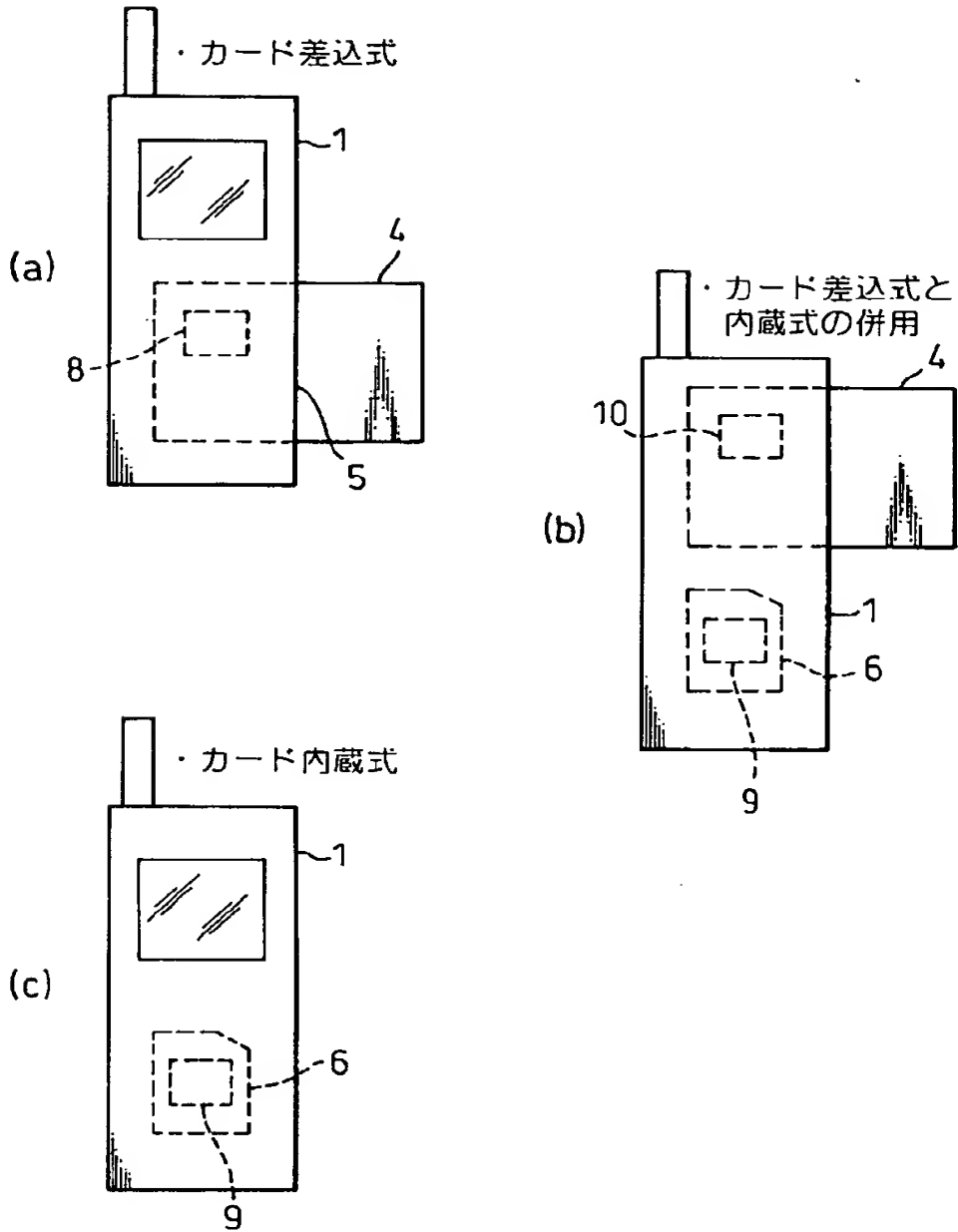
携帯情報端末



【図 2】

図 2

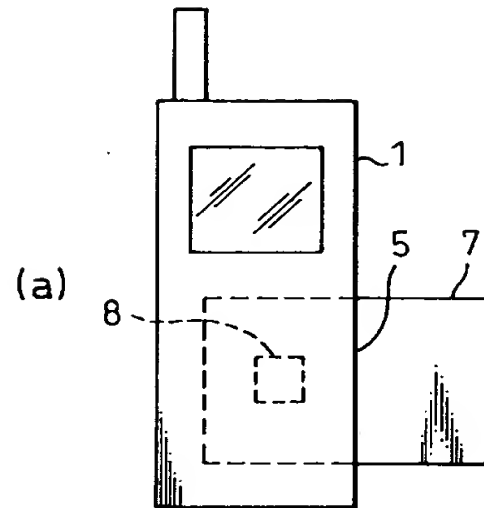
接触型 I C カード R / W を内蔵



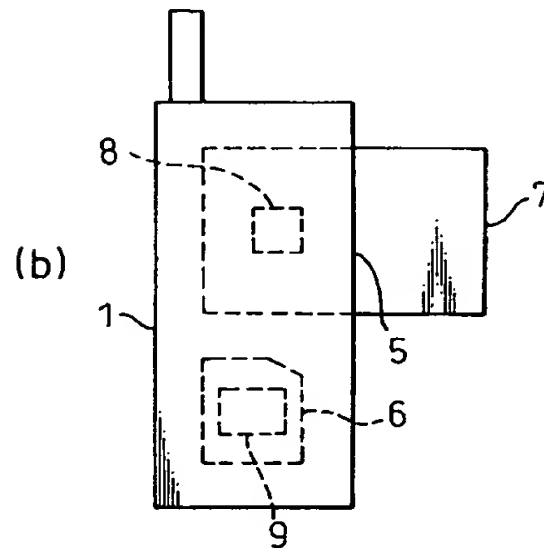
【図3】

図3

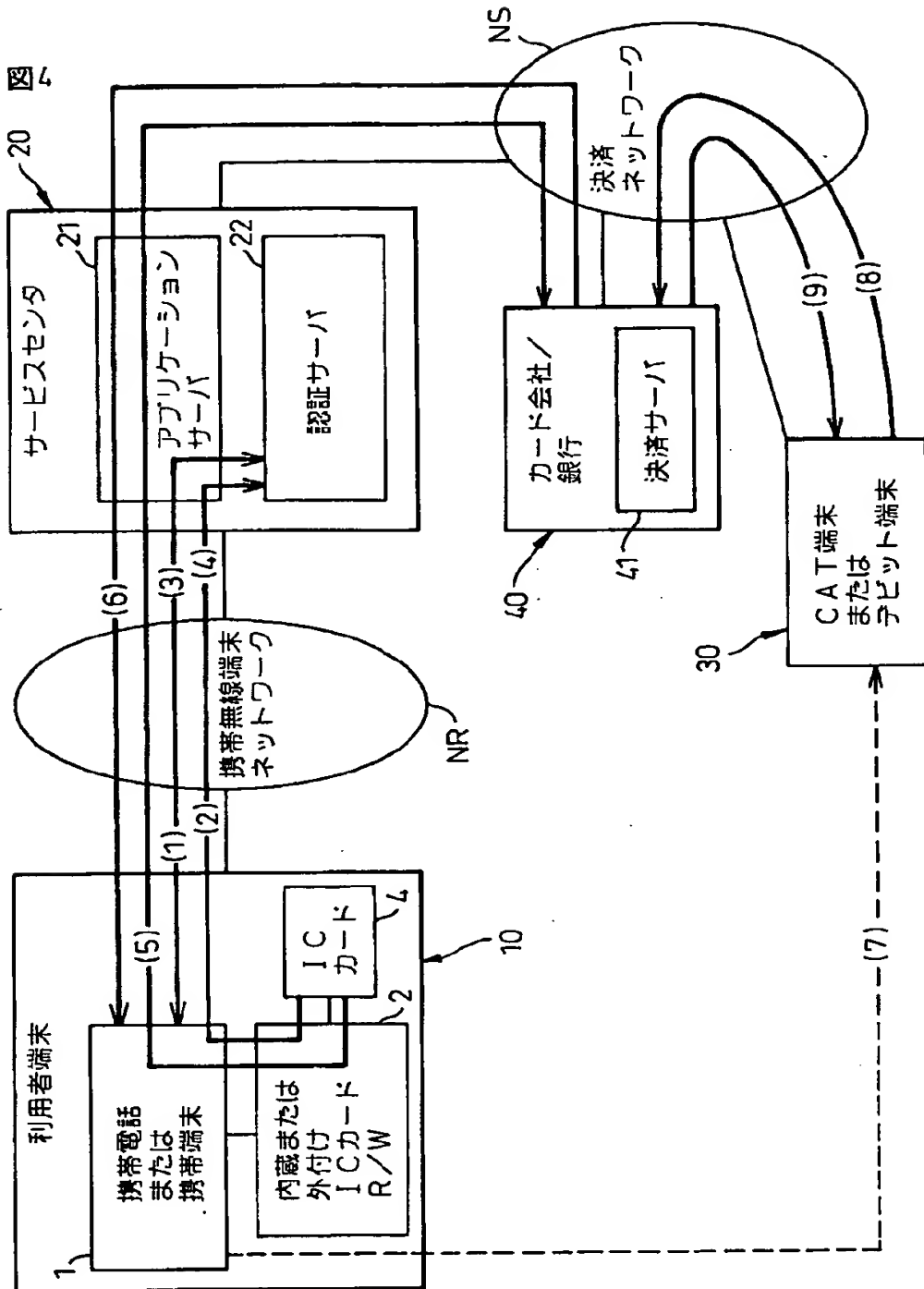
非接触型 ICカード R/W を内蔵



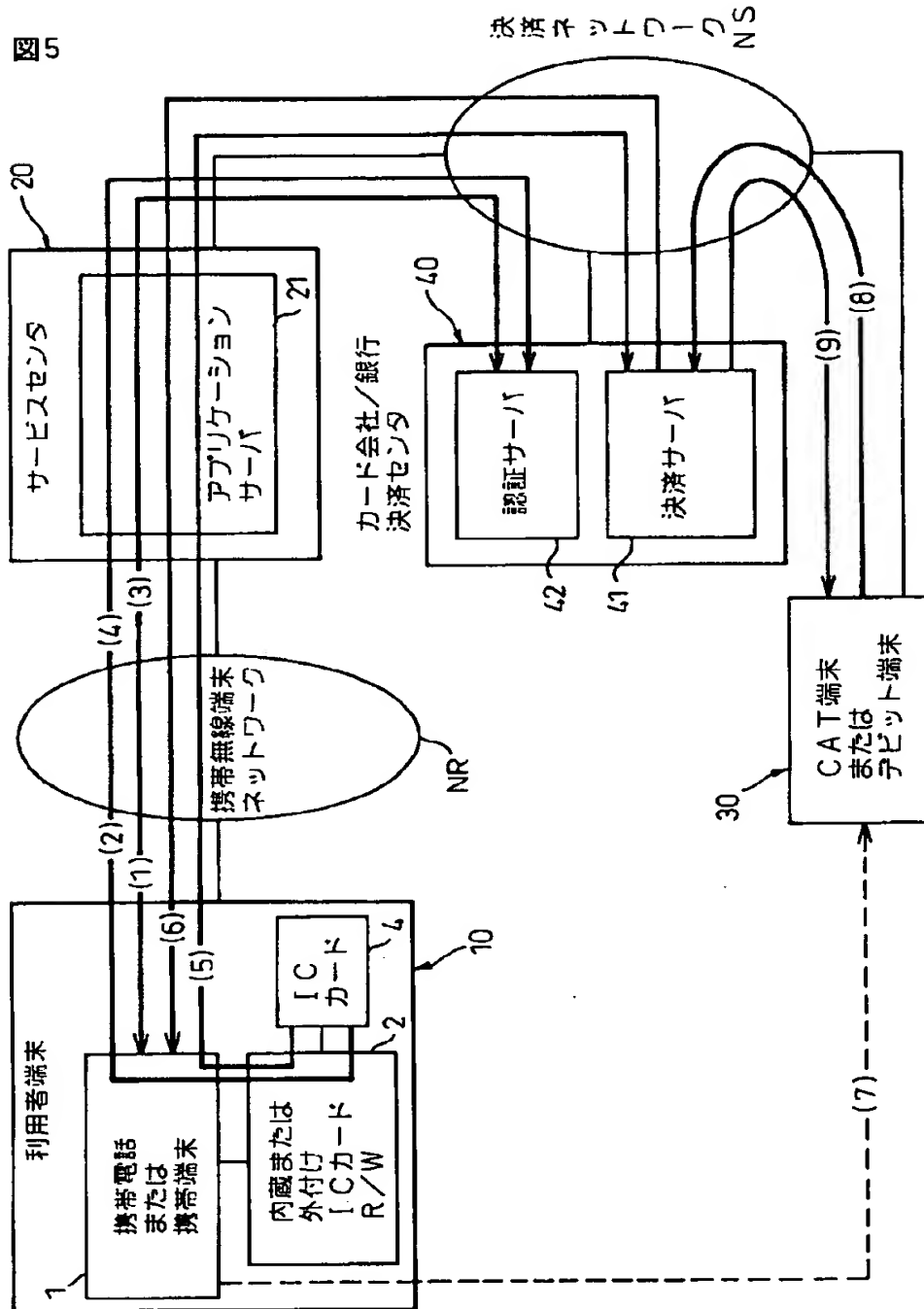
接触型 ICカード R/W と  
非接触型 ICカード R/W の両方を内蔵



【図 4】

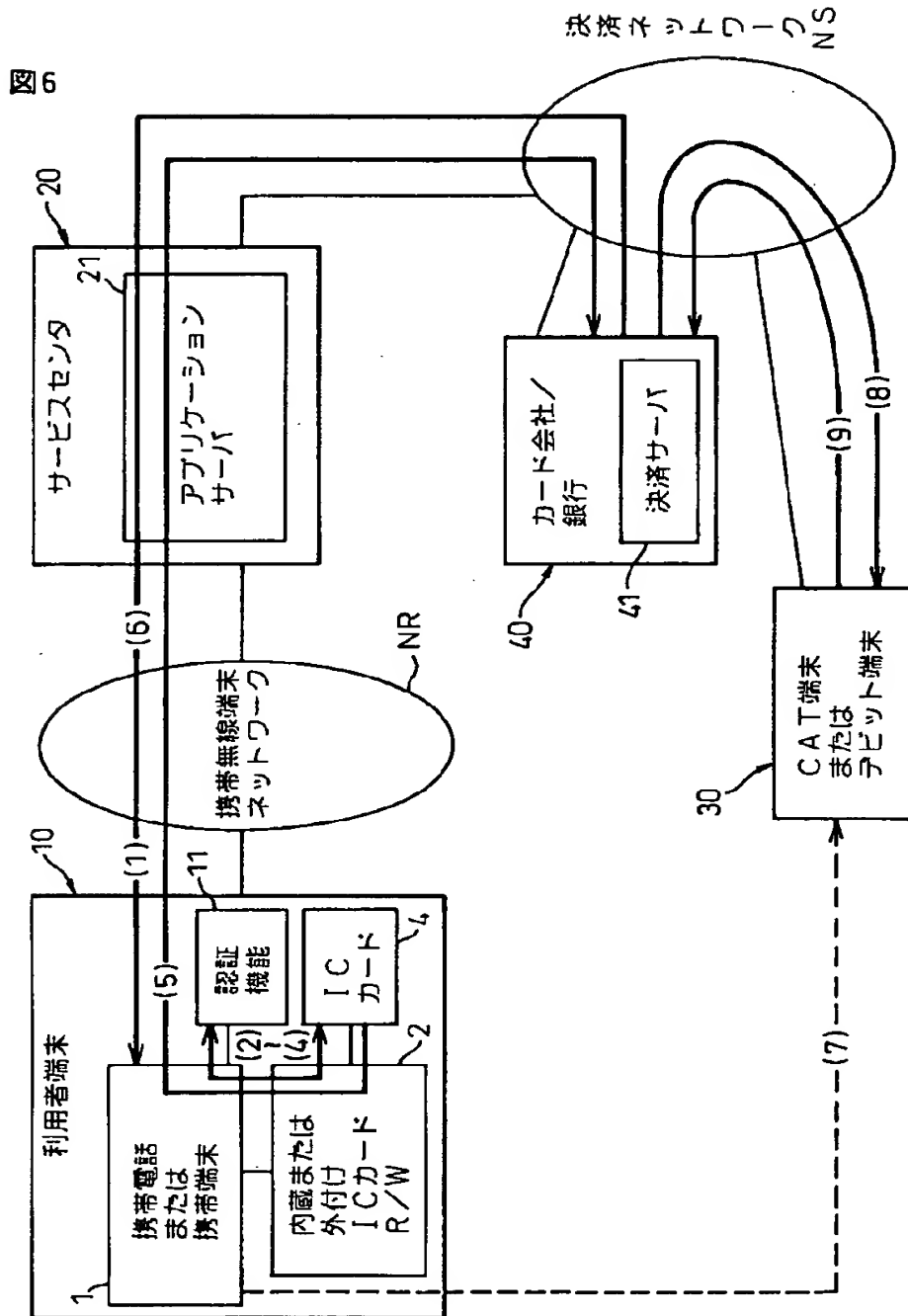


【図 5】

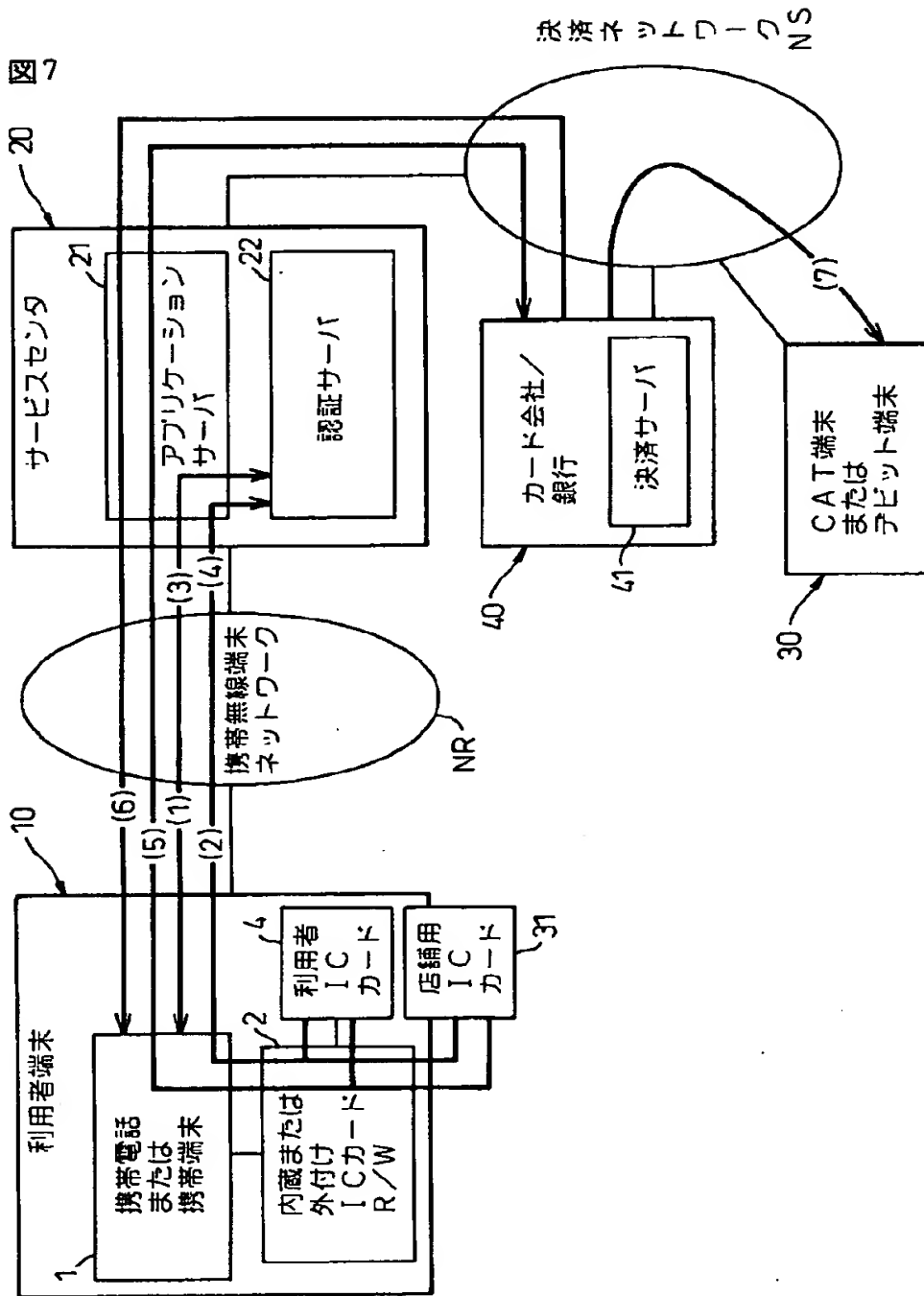


【図6】

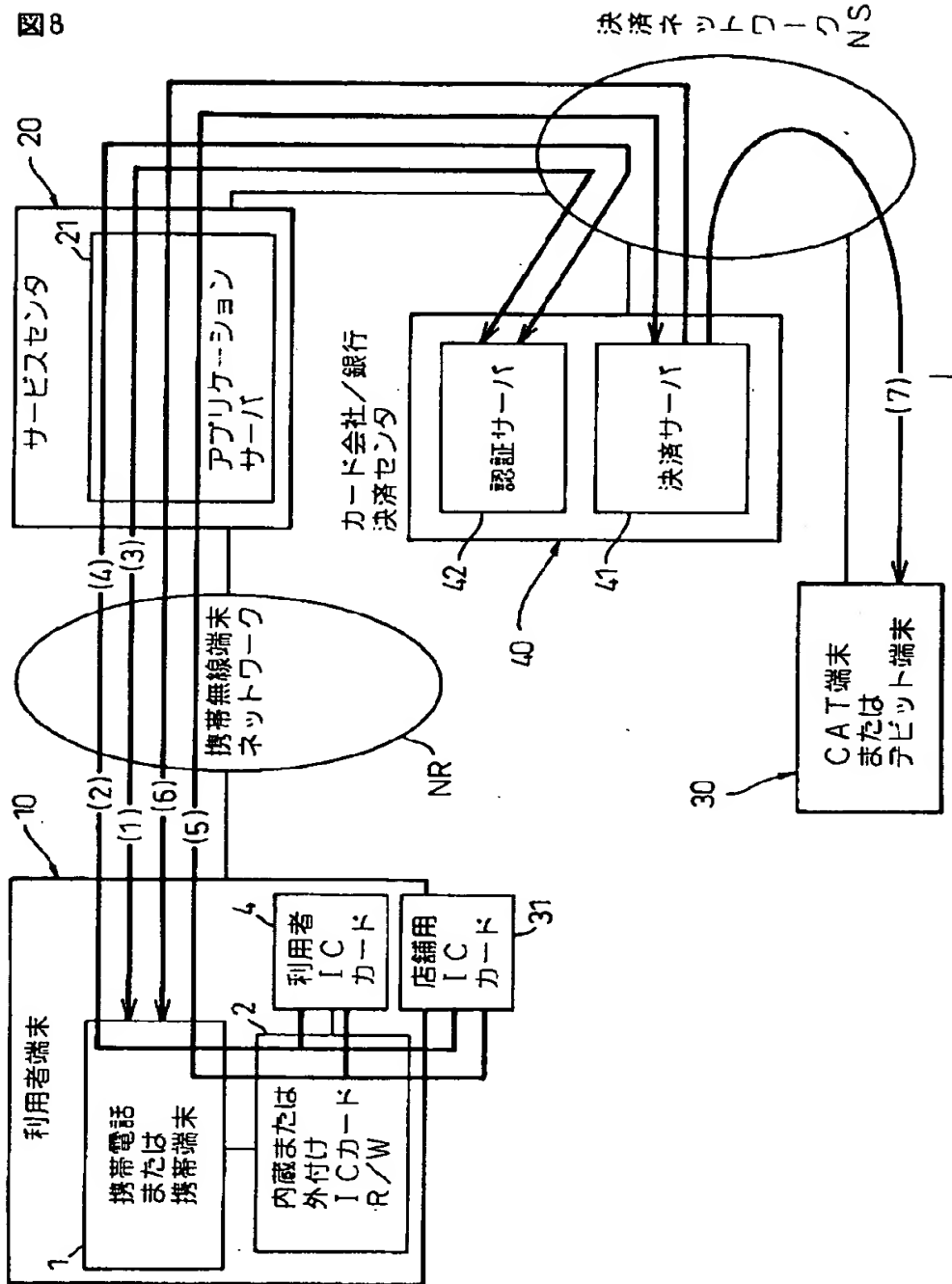
携帯端末の内部に認証機能を持つ場合



【図 7】

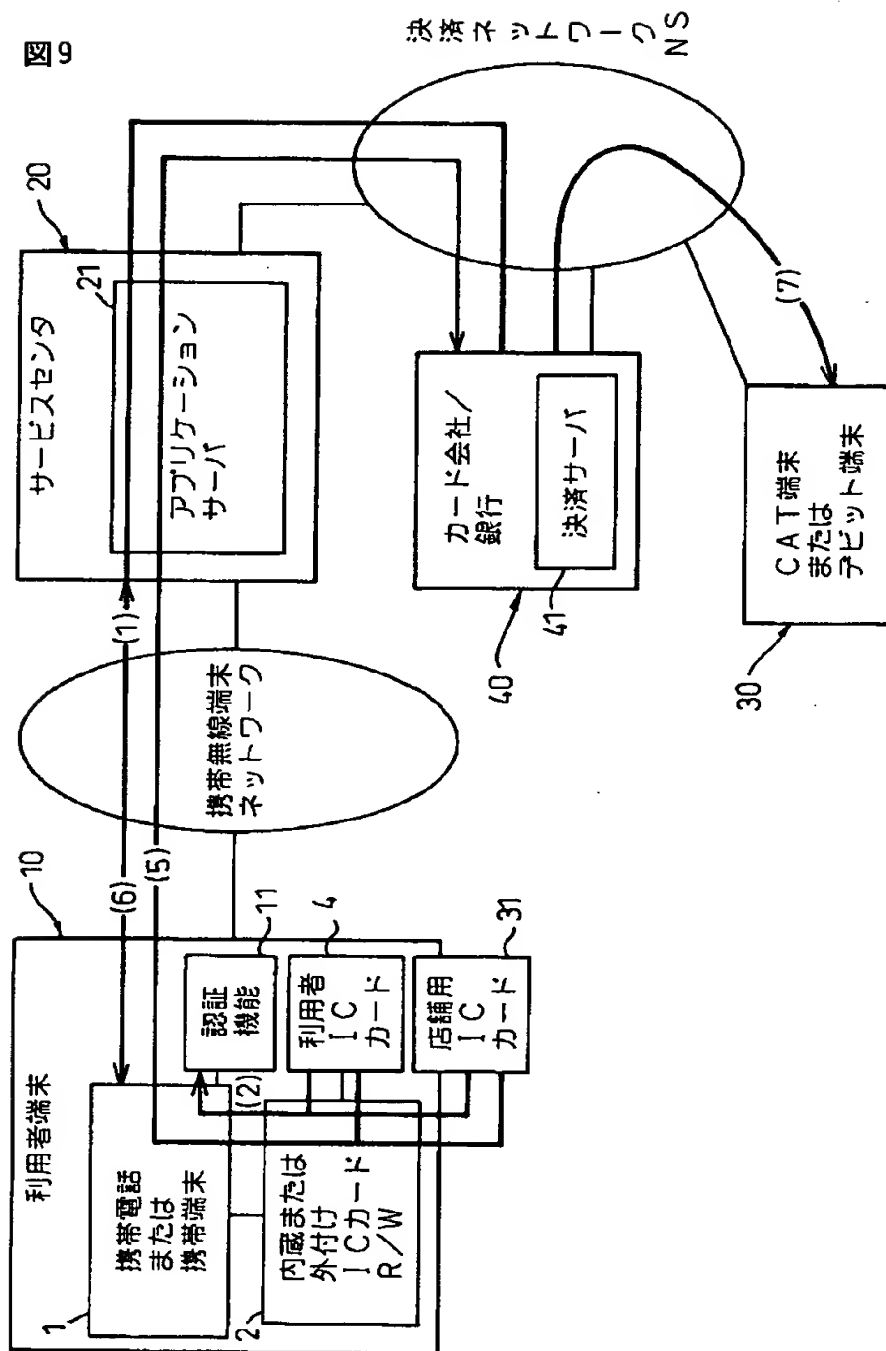


【図 8】



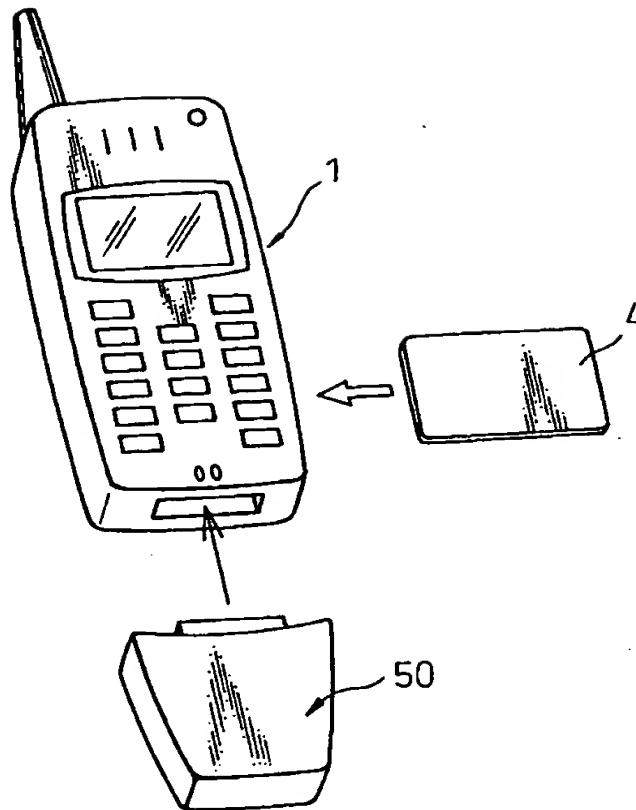


【図 9】



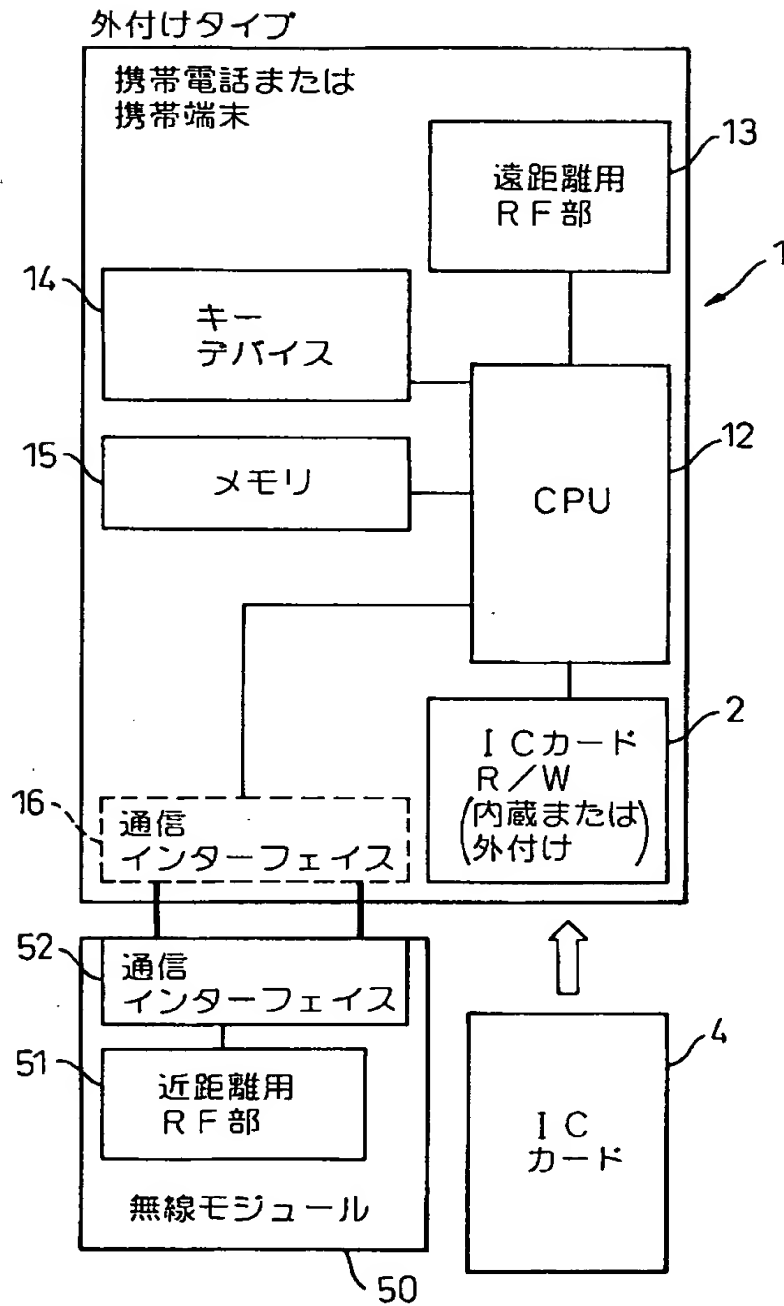
【図 1 0】

図 10



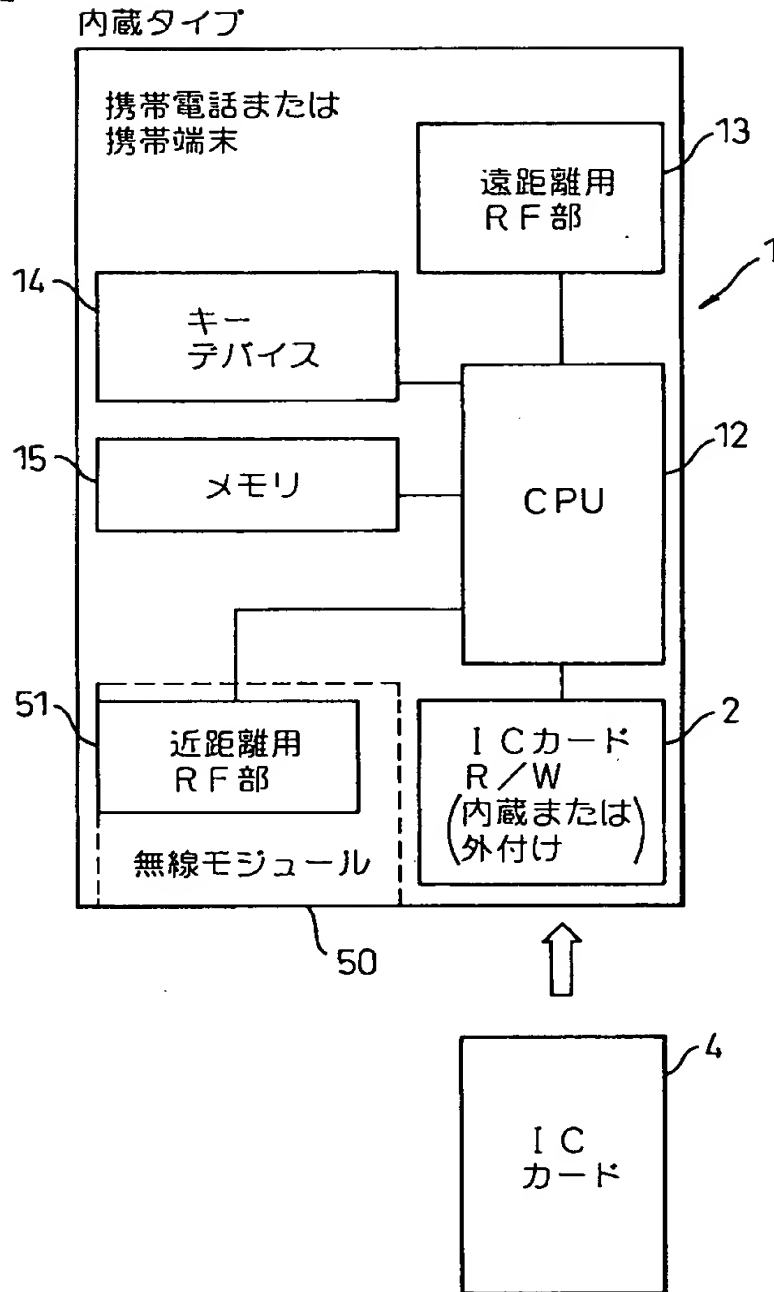
【図 1 1】

図 11

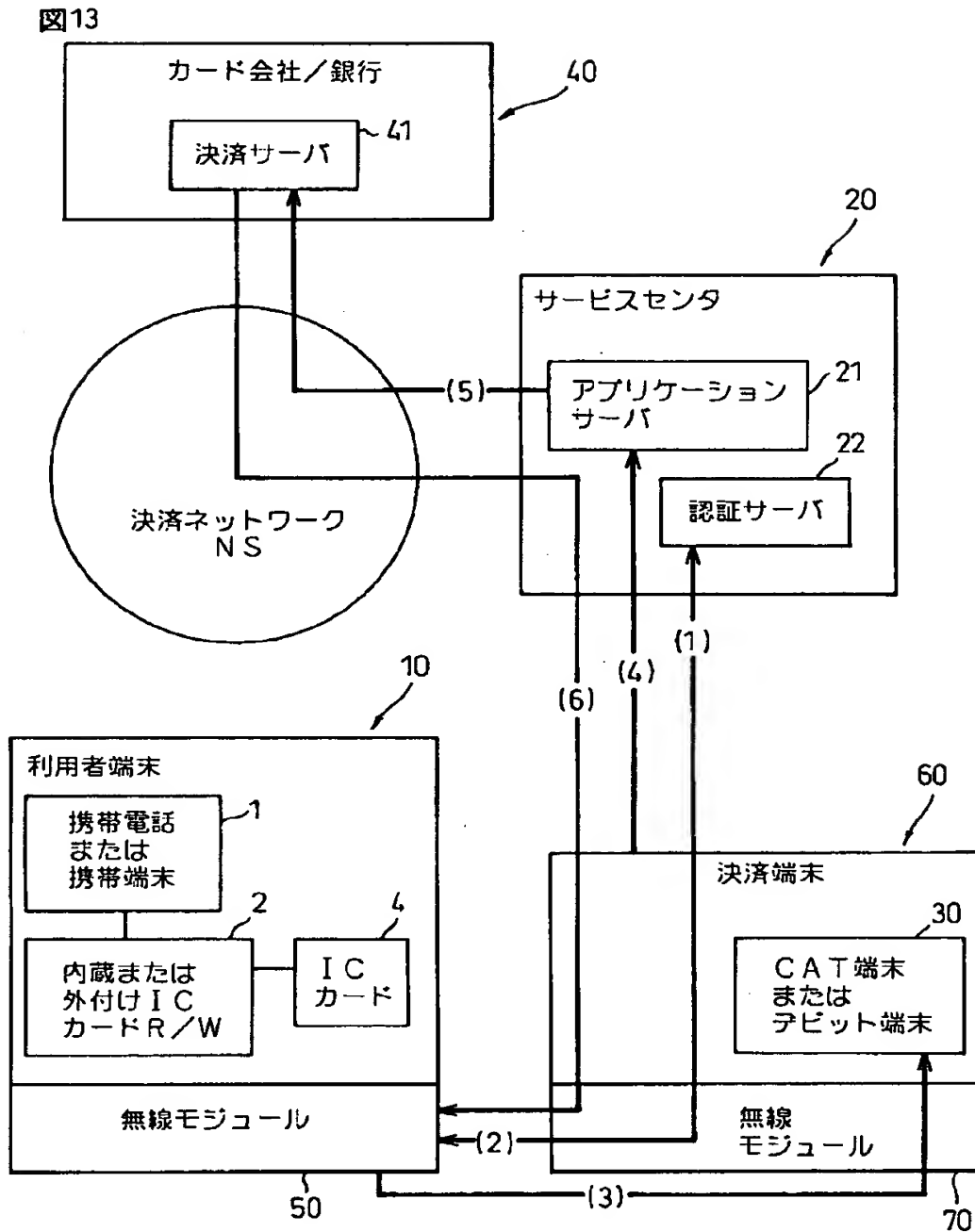


【図 12】

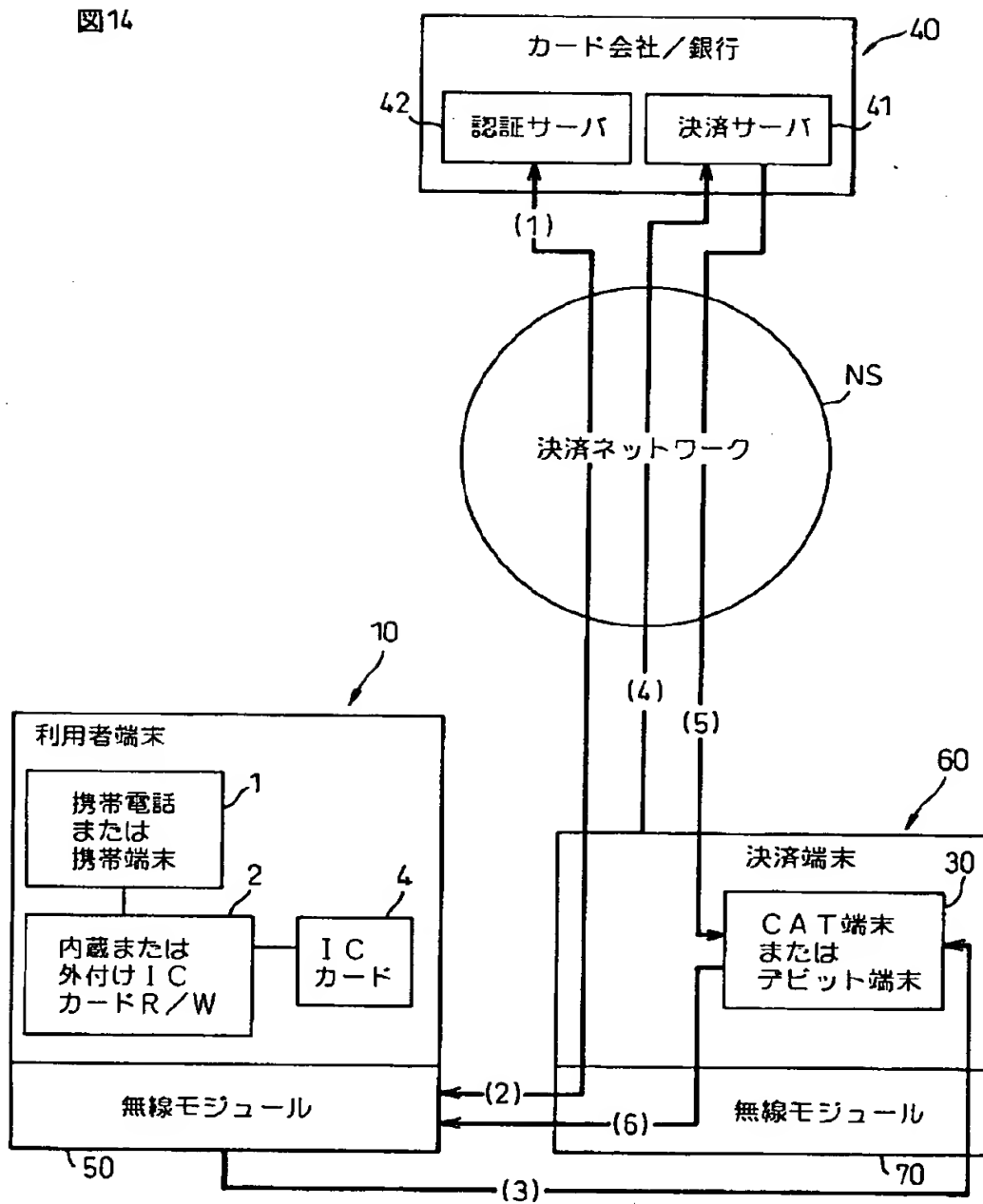
図12



【図13】

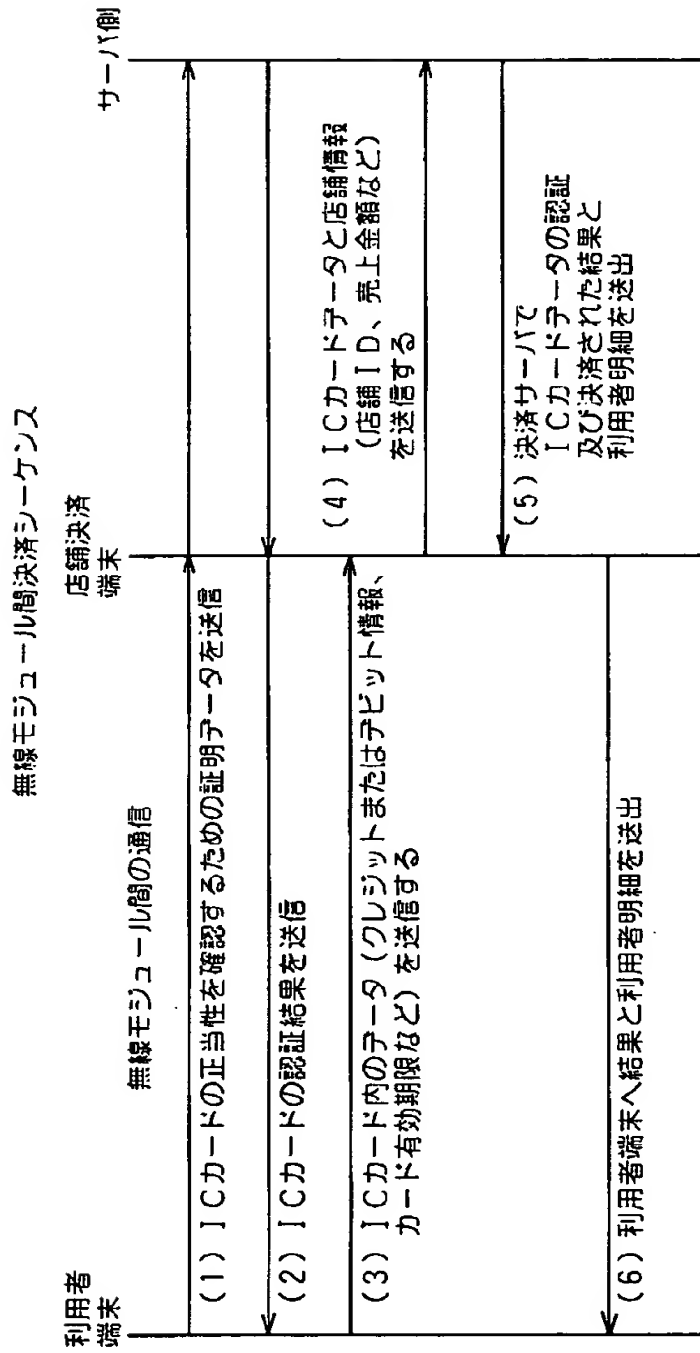


【図14】



【図 15】

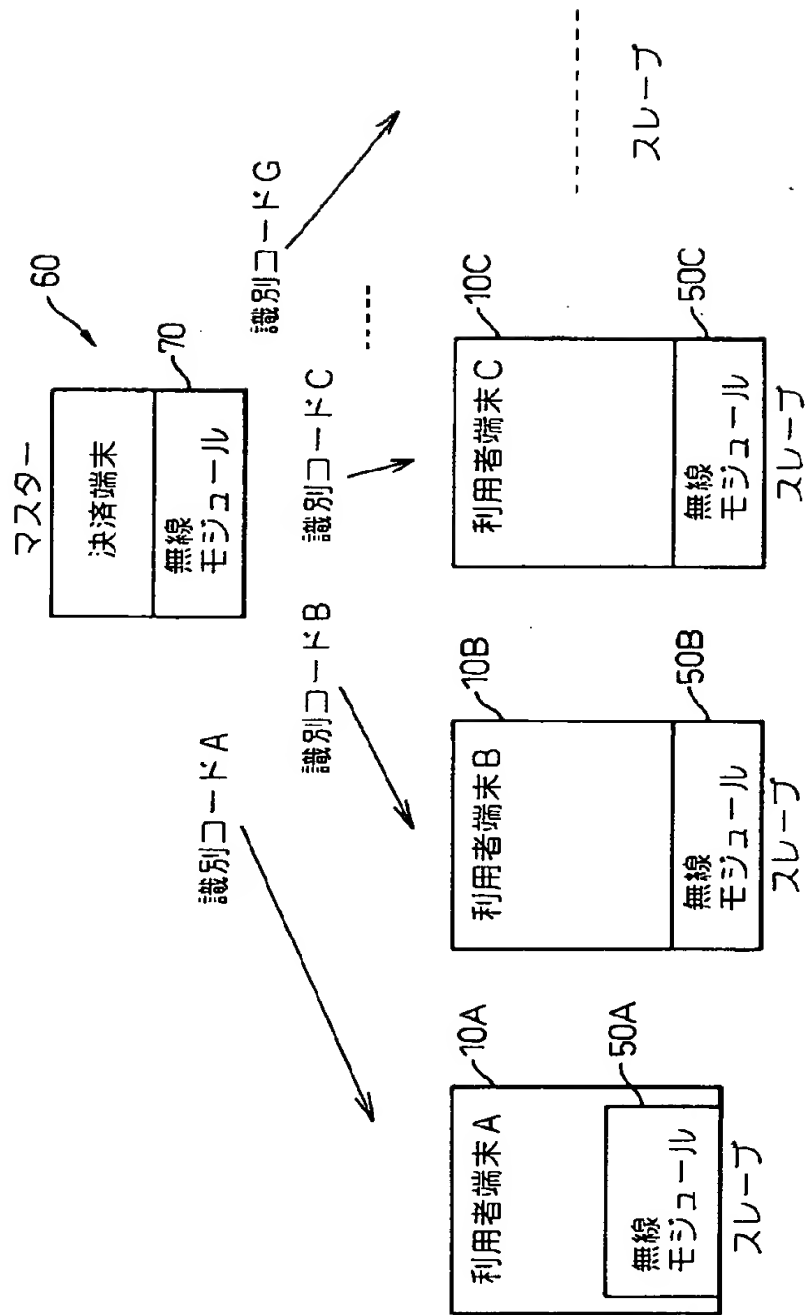
図15



\* 無線モジュール間のデータは、利用する無線プロトコルの暗号方式を利用して暗号化する

【図 16】

図 16





【書類名】 要約書

【要約】

【課題】 ICカード読み書き機能の付いた携帯情報端末を利用して、決済機能付のICカードによる決済サービスを実現させて利便性を図る。

【解決手段】 既存のカード決済システムに加えて、ICカードの読み書き可能な携帯情報端末1と、携帯情報端末のネットワークNRと決済ネットワークNS間のゲートウェイ機能を提供するアプリケーションサーバ21を設け、店舗において顧客がICカード4を装着した携帯情報端末1からアプリケーションサーバ21経由で認証サーバ22に接続して認証情報とクレジット情報を認証サーバ22に送出し、認証サーバ22がICカード4の適否を認証した後、クレジット情報に基づいて作成したワンタイムパスワードを携帯情報端末1の表示器に表示させ、店舗側がこのワンタイムパスワードと売上情報を決済端末30から入力して決済が完了するシステムである。

【選択図】 図4

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社